Symantec™ Server Management Suite 8.1 powered by Altiris™ technology Release Notes

Symantec™ Server Management Suite 8.1 powered by Altiris™ technology Release Notes

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our website at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information

- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

support.symantec.com

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apj@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Server Management Suite 8.1

This document includes the following topics:

About Server Management Suite

Server Management Suite combines the essential tools that help you manage your physical and virtual servers, reduce service interruptions, and increase uptime.

Server Management Suite incorporates a variety of features that let you automate configuration, stage tasks, and create policies to manage your servers. Graphical reports let you quickly identify the health of your environment, pinpoint problems,

and analyze trends. Expanded support for virtual technologies simplifies the management of multiple operating system environments.

Server Management Suite is a collection of solutions that run on the Symantec Management Platform that provides the following key features:

- Discovery and inventory
  The suite automatically identifies the devices that are found in your network, and collects inventory data across your environment. Multi-platform support consolidates the discovery data of all Windows, UNIX, and Linux assets within an integrated console. You can easily assess security vulnerabilities, prepare for software audits, and more accurately determine hardware availability and needs.
- Provisioning
  The suite lets you improve the consistency and increase the quality of server configurations. It delivers deployment capabilities that include image-based or scripted operating system installation and continuous provisioning. The suite helps you implement the standardized configurations and provides the tools for migration.
- Software distribution and patch management
  The suite lets you control server configurations through its software management capabilities. Automated policies for software and patch management help you keep the servers standardized and secure. You can modify similar configurations on multiple servers simultaneously. You can distribute applications, and security updates to target systems.
- Proactive monitoring and alerting
  The suite helps you monitor the critical components of your network. You can increase the network uptime with the remediation tasks that are configured before the critical events occur. You can organize your servers into vital groups and quickly ascertain the current health of the whole network. The monitoring capabilities provide a summarized view of each single-server performance over time.

See “Components of Server Management Suite” on page 7.

See “Where to get more information” on page 92.

Components of Server Management Suite

Server Management Suite is a collection of solutions that run on the Symantec Management Platform. These solutions let you discover, inventory, monitor, and provision servers from a central console - the Symantec Management Console.

See “About Server Management Suite” on page 6.

Table 1-1 Components of Server Management Suite

Component	Description	Link to User Guide
Symantec Management Platform	Symantec Management Platform provides a set of services that IT-related solutions can leverage. By leveraging these services, the solutions that are built on the platform can focus on their unique tasks. They also can take advantage of the more general services that the platform provides. The platform services also provide a high degree of consistency between the solutions, so that users do not need to learn multiple product interfaces. Symantec Management Platform provides the following services: ■ Role-based security ■ Client communications and management ■ Execution of scheduled or event-triggered tasks and policies ■ Package deployment and installation ■ Reporting ■ Centralized management through a single, common interface Symantec Management Platform includes the following components: ■ Configuration Management Database (CMDB) ■ Notification Server ■ Symantec Management Console ■ Symantec Management Agent for Windows ■ Symantec Management Agent for UNIX, Linux, and Mac ■ Network Discovery ■ Software Management Framework	DOC9469

Table 1-1 Components of Server Management Suite *(continued)*

Component	Description	Link to User Guide
Deployment Solution	Deployment Solution helps to reduce the cost of deploying and managing servers, desktops, and notebooks from a centralized location in your environment. It offers operating system deployment, configuration, personality migration of computers, and software deployment across different hardware platforms and operating systems. Deployment Solution provides integrated, disk imaging, and personality migration from the Symantec Management Console. Using Symantec Ghost™, you can perform initial computer deployment using standard images and migrate user data and application settings to new computers. For the Deployment Solution release notes, see the link at the following URL: http://www.symantec.com/docs/DOC9583	DOC9496
ITMS Management Views	ITMS Management Views replace the default console views for computers and software that existed in Symantec Management Platform version 7.0. For tasks and policies, the Management views add drag-and-drop functionality. In addition, you can now search the tree rather than drilling down to find specific tasks or policies. The Management views are incorporated into the existing console. For more information, see the *IT Management Suite Administration Guide*.	DOC9469

Table 1-1 Components of Server Management Suite *(continued)*

Component	Description	Link to User Guide
Inventory Solution	Inventory Solution lets you gather inventory data about the computers, users, operating systems, and installed software applications in your environment. You can collect inventory data from the computers that run Windows, UNIX, Linux, and Mac. After you gather inventory data, you can analyze it using predefined or custom reports. For example, you can gather information for all the Symantec Endpoint Protection Windows and Mac clients that are installed on managed and unmanaged computers in your environment. Then you can view the gathered data in the Resource Manager or in the **Computers** Management view, in the **SEP Agent** summary flipbook.	DOC9616
Inventory Pack for Servers	Inventory Pack for Servers gathers server-based inventory data from servers that run Windows, UNIX, and Linux. It runs on top of Inventory Solution and uses the same Inventory plug-ins, tasks, and wizards.	DOC9616
Inventory for Network Devices	Inventory for Network Devices gathers inventory data from the devices that are not managed through the Symantec Management Agent. You can gather inventory on the devices that are already discovered and exist as resources in the CMDB.	DOC9605
Monitor Solution for Servers	Monitor Solution for Servers lets you monitor various aspects of computer operating systems, applications, and devices. These aspects can include events, processes, and performance. This ability helps you ensure that your servers and your devices work and reduces the costs of server and network monitoring.	DOC9587
Monitor Pack for Servers	Monitor Pack for Servers works with the Monitor Solution core components of the Symantec Management Platform. It lets you monitor operating system performance, services, and events of your Windows, UNIX, and Linux server environment.	DOC9587

Table 1-1 Components of Server Management Suite *(continued)*

Component	Description	Link to User Guide
Patch Management Solution	Patch Management Solution for Linux lets you scan Red Hat and Novell Linux computers for security vulnerabilities. The solution then reports on the findings and lets you automate the download and distribution of needed errata, or software updates. The solution downloads the required patches and provides wizards to help you deploy them. Patch Management Solution for Mac lets you scan Mac computers for the updates that they require. The solution then reports on the findings and lets you automate the downloading and distribution of needed updates. You can distribute all or some of the updates. Patch Management Solution for Windows lets you scan Windows computers for the updates that they require, and view the results of the scan. The system lets you automate the download and distribution of software updates. You can create filters of the computers and apply the patch to the computers that need it.	■ Patch Management Solution for Linux: DOC9606 ■ Patch Management Solution for Mac: DOC9607 ■ Patch Management Solution for Windows: DOC9608
Real-Time System Manager	Real-Time System Manager provides you detailed real-time information about a managed computer, and lets you remotely perform different administrative tasks in real time. Real-Time System Manager also lets you run some of the management tasks on a collection of computers. You can run the tasks immediately, or on a schedule.	DOC9304

Table 1-1 Components of Server Management Suite *(continued)*

Component	Description	Link to User Guide
Software Management Solution	Software Management Solution provides intelligent and bandwidth-sensitive distribution and management of software from a central web console. It leverages the Software Catalog and Software Library to ensure that the required software gets installed, remains installed, and runs without interference from other software. Software Management Solution supports software virtualization technology, which lets you install software into a virtual layer on the client computer. Software Management Solution also lets users directly download and install approved software or request other software.	DOC9609
Virtual Machine Management	Virtual Machine Management helps you to view virtual resource information in your network and perform management tasks on those virtual resources. You can create virtual environments of servers, storage devices, and network resources on a single physical server. Each virtual environment is isolated and functions independently from the physical server and from the other virtual environments. Virtualization enhances the efficiency and productivity of the hardware resources and helps to reduce administrative costs.	DOC9627

Table 1-1 Components of Server Management Suite *(continued)*

Component	Description	Link to User Guide
Symantec Workflow Solution	Symantec Workflow is a security process development framework that you can use to create both automated business processes and security processes. These processes provide for increased repeatability, control, and accountability while reducing overall workload. The Symantec Workflow framework also lets you create Workflow processes that integrate Symantec tools into your organization's unique business processes. Once deployed, Symantec Workflow processes can respond automatically to environmental variables. Symantec Workflow processes can also allow for human interface points when a process calls for someone to make a decision with accountability. For the Symantec Workflow Solution release notes, see the link at the following URL: http://www.symantec.com/docs/DOC9624	DOC9625
Topology viewer	Topology viewer is a Web Part on the **Server Management Portal** page that provides a network topology diagram of the SNMP-enabled devices that are found in your network.	N/A
Server Resource Manager Home page	The **Server Resource Manager Home** page consolidates the most relevant inventory and monitoring data of a server resource into a single view.	N/A

What's new in Server Management Suite 8.1

In Server Management Suite 8.1, new features for the following solutions and components are introduced:

- Symantec Management Platform
  See "What's new in Symantec Management Platform" on page 14.
- Deployment Solution
  See "What's new in Deployment Solution" on page 20.
- Inventory Solution
  See "What's new in Inventory Solution" on page 21.
- ITMS Management Views

See "What's new in ITMS Management Views" on page 22.

- Patch Management Solution
  See "What's new in Patch Management Solution" on page 23.
- Real-Time System Manager Solution
  See "What's new in Real-Time System Manager Solution" on page 25.
- Software Management Solution
  See "What's new in Software Management Solution" on page 25.
- User Documentation
  See "What's new in User Documentation" on page 26.
- Virtual Machine Management
  See "What's new in Virtual Machine Management" on page 27.
- Workflow Solution
  See "What's new in Workflow Solution" on page 27.

What's new in Symantec Management Platform

In the Symantec Management Platform 8.1, the following new features are introduced:

Table 1-2 List of new features

Feature	Description
Expanded list of supported platforms for CMDB.	The following version(s) of Microsoft® SQL Server® are now supported for the Configuration Management Database (CMDB): ■ SQL Server® 2012 SP3 ■ SQL Server® 2014 SP2 ■ SQL Server® 2016

Table 1-2 List of new features *(continued)*

Feature	Description
Expanded list of supported platforms for Symantec Management Agent.	The following operating systems are now supported for the installation of the Symantec Management Agent: ■ CentOS 6.0 - 6.8 and CentOS 7.0 - 7.2 For the list of supported solutions and limitations, refer to: http://www.symantec.com/docs/DOC9725 ■ AIX 7.1 TL4 For the list of supported solutions and limitations, refer to: http://www.symantec.com/docs/HOWTO125360 ■ macOS 10.12 Sierra For the list of supported solutions and limitations, refer to: http://www.symantec.com/docs/HOWTO125347 ■ RHEL 6.7 For the list of supported solutions and limitations, refer to: http://www.symantec.com/docs/DOC9268 ■ RHEL 6.8 For the list of supported solutions and limitations, refer to: http://www.symantec.com/docs/HOWTO125430 ■ RHEL 7.2 For the list of supported solutions and limitations, refer to: http://www.symantec.com/docs/HOWTO124979 ■ Solaris 11.3 For the list of supported solutions and limitations, refer to: http://www.symantec.com/docs/HOWTO124985 ■ SUSE Linux Enterprise 12 SP1 For the list of supported solutions and limitations, refer to: http://www.symantec.com/docs/HOWTO124980 ■ Windows 10 Anniversary Update 1 (Windows 10, version 1607) For the list of supported solutions and limitations, refer to: http://www.symantec.com/docs/HOWTO125345 ■ Windows Server 2016 For the list of supported solutions and limitations, refer to: http://www.symantec.com/docs/HOWTO125454

Table 1-2 List of new features *(continued)*

Feature	Description
Peer-to-peer downloading.	The peer-to-peer downloading feature lets you download and distribute the software delivery and patch packages to Windows computers. It minimizes the software delivery time and provides you with a reliable software delivery to all endpoints. The peer-to-peer downloading feature significantly reduces the load on the network and the IT Management Suite infrastructure. For more information about peer-to-peer downloading, see the knowledge base article at the following URL: http://www.symantec.com/docs/DOC9473
Data migration between different versions of Symantec Management Platform.	Standalone replication and data export/import is now supported between Notification Servers that have different versions of IT Management Suite installed. Note that you can only replicate or export/import data from IT Management Suite version 7.6 HF7 or version 8.0 HF6 to IT Management Suite 8.1. For more information about data migration, see the knowledge base article at the following URL: http://www.symantec.com/docs/DOC9586
The licenses in SLIC format are now supported.	The licensing for ITMS functions now as follows: ■ The licenses in SLIC format are only supported for ITMS version 8.1. The import of SLIC license files for ITMS versions earlier than 8.1 is rejected. ■ Applying new SLIC license overwrites the existing legacy licenses. Note that even valid legacy licenses get overwritten. If you need to extend the node count for current legacy license for 8.1 product, Symantec issues a replacing SLIC license with new extending licenses. For example, if you want to extend license from 300 to 400 nodes - you get replacing SLIC license for 300 nodes and additional license for 100 nodes. ■ If multiple license files are applied for a single solution, each SLIC license is displayed in a separate row. ■ Adding new SLIC license on top of existing valid SLIC license adds nodes to the sum of allowed nodes. If you have any questions about SLIC licenses, contact the Symantec Customer Care.

Table 1-2 List of new features *(continued)*

Feature	Description
Mac OS Profile Management.	Mac OS Profile Management feature lets you import Mac configuration profiles and enforce them by implementing policies. Configuration profiles let you configure settings such as email settings, network settings, or distribute certificates to Mac computers. **Note:** This feature is only available if you install Client Management Suite 8.1 For more information about Mac OS Profile Management, see the knowledge base article at the following URL: http://www.symantec.com/docs/HOWTO125782
New features in SIM.	SIM introduces the following new features: ■ To increase security, XML signing for PL is implemented. Note that no limitations to functionality apply, only warning is displayed. ■ Database configuration has been moved from Symantec Management Console to SIM. This helps to troubleshoot database issues even when the Console is inaccessible. ■ Performing full repair is implemented. Full repair verifies the connection to the CMDB, repairs the installation errors, and reconfigures the installed solutions and components. ■ Repairing MSI-s and reconfiguring installed solutions is moved to separate pages to simplify the user interface.
Enhancements of target selector for policies and tasks.	■ From the **Apply to** menu, you can access to the recently used targets. ■ Saved targets are re-usable and editable by users with the same scope of access. ■ It is possible to view and edit the target scoping. ■ For computers target, you can include or exclude the unmanaged computers.
Prerequisites displayed for Task Service and Package Service.	In the **Add/Remove Services** dialog box, you can now right-click the service and view the list of prerequisites for installing this service.
UI enhancements on the **Site Server Settings** page.	The following changes have been made on the **Site Server Settings** page: ■ Task Server with version older than the version of Task Management installed on Notification Server has now status **Warning/Required Upgrade**. ■ Major information about the Task Server is now displayed under **Task Service** section. ■ Right-click menu now works similarly to other Symantec Management Console pages.

Table 1-2 List of new features *(continued)*

Feature	Description
UI enhancements in **Security Role Manager** and on the **Automation Policies** page.	The following changes have been made in **Security Role Manager**: ■ Enhanced **View** and **Search** options to simplify finding the required item. ■ Extended layout to provide more information for the selected item. The following changes have been made on the **Automation Policies** page: ■ The state of each automation policy is indicated more clearly. ■ New system messages available. ■ New override and filtering options for system messages.
Added possibility to select multiple tasks when creating a job.	When you create a job and add tasks to it, you can now select multiple tasks at once by holding down the **Ctrl** key.
Possibility to prevent computer from going into sleep mode while task runs.	If a computer goes to sleep mode while a task runs on it, the task will fail. To fix this issue, you can now prevent the computer from going to sleep mode by enabling the **Prevent the computer from going into sleep mode while the tasks run** option at the following locations: ■ On the **Task Agent Settings** page (global settings) ■ In the advanced options dialog box, on the **Task options** tab, of a client task. Note that for **Defragment Computer** task, this option is enabled by default.
Non-English job's conditions now work with localized **True/False**.	It is now possible to use localized **True/False** strings in job's conditions and they function as expected. Note that the change affects only the jobs that are created after the upgrade. The jobs that are created before the upgrade will function as previously.
Search in **Create New Task** and **Select Task** dialog box.	In the **Create New Task** dialog box and **Select Task** dialog box, it is now possible to use search.
New configuration option is added to the **Cleanup Task Data** task.	In the environment with high task load, the **Cleanup Task Data** task may remove the task instances of the recently executed tasks. As a result, some task instances might be missing and the summary information for that task may be incorrect. To avoid this problem, you can now enable the **Minimum time period to keep the task instances/summaries** option. If you enable this option, the **Cleanup Task Data** task will not remove the task records that are newer than the defined time period.

Table 1-2 List of new features *(continued)*

Feature	Description
The defer dialog box for the tasks is redesigned.	After you enable the option **Allow the user to defer execution of this task** in the Symantec Management Console, a defer dialog box is displayed on the client computer that allows the user to postpone the task. This defer dialog box is now redesigned. The redesign addresses multiple stability and usability issues.
Added ability to assign multiple packages to specific Package Servers.	On the **Packages** page, you can select multiple packages and assign these packages simultaneously to all Package Servers or to specific Package Servers.
Altiris Client Task Server Agent plug-in has been optimized.	As a result of optimization, the 32-bit version of the `CTServerAgent.dll` is not installed on a 64-bit operating system. In the Symantec Management Agent UI, on the **Agent Settings** tab, under **Agents/Plug-ins**, only one record is displayed for the Altiris Client Task Server Agent plug-in.
New **Client Task Status Details** report is available.	The new **Client Task Status Details** report displays details of a specific task or job. For example, you can view the list of computers on which this task or job was launched. To access the report, double-click any task or job item in the **Job/Task Status Detail** report. The **Job/Task Status Detail** report is located in the Symantec Management Console, at **Reports > Task Server > Status > Job/Task Status Detail**.
New reports are introduced on internal health indication.	The following new reports are available: ■ **Notification Server Processes Statistics** report This report shows the statistics of the Altiris processes for this Notification Server. You can drill down each record to see the detailed resource usage data of an Altiris process within certain time range. ■ **Client Configuration Policy Statistics** report This report shows the history of the policies requests that the managed computers have made on this Notification Server.
Added possibility to generate bootstrap files using the custom configuration XML.	You can now also apply custom settings to ULM agent pull installation packages and to ULM agent Cloud-enabled installation packages using the custom configuration XML.
Added possibility to perform actions on multiple items in the search results list.	In the Symantec Management Console, you can now select multiple items in the search results list and perform actions on them. For example, you can select multiple policies in the search results list, and then enable or disable them at once.

Table 1-2 List of new features *(continued)*

Feature	Description
Redirecting 8.0 HF1 Mac agents to 8.1 Notification Server.	Starting from ITMS version 8.0HF1, you can use Communication Profiles to redirect cloud-enabled Mac agents to Notification Server 8.1. For more information about restoring Cloud-enabled Management communication on Mac computers after an off-box upgrade, see the *IT Management Suite 8.1 Installation and Upgrade Guide*: http://www.symantec.com/docs/DOC9500
Smart Card Authentication for Symantec Management Console.	For more information about how to configure Smart Card Authentication for Symantec Management Console, see the following knowledge base article: http://www.symantec.com/docs/DOC9334

What's new in Deployment Solution

In Deployment Solution 8.1, the following new features are introduced:

Table 1-3 List of new features

Feature	Description
Enhanced Resource Import tool.	The Resource Import tool now lets you import an image as an external package to remote site servers. **Note:** Currently, the tool cannot cycle through different drives when there is no disk space.
WinPE 10 (version 1511) support.	Deployment Solution now supports WinPE 10 (version 1511) preboot configuration. For more information, refer to the following article: INFO3561
Support for 4K drive.	Deployment Solution now supports storing images on external 4K USB hard drives. **Note:** Scripted OS install is not supported for a 4K drive.
Deploy Image task is updated.	The default value of the **Bypass Driver Validation** option is now set to **All** in the **Deploy Image** task.
Enhanced image storage on Site servers.	Resource Import Tool on a package server can import images without installing the Deployment Solution Task Service on the same server.
Support for XFS file system on RHEL 7.	Deployment Solution now supports provisioning RHEL 7 computers with XFS file system.

Table 1-3 List of new features *(continued)*

Feature	Description

Updated task for uploading files.	For the following deployment tasks, if you want to upload more than one file, you must upload the files only when you include all the files in a folder and compress it into a single zip file:
	■ **Copy File**
	■ **OS Files: Add Files**
	■ **Driver management**
	■ **Add Preboot Configuration > Select Mac Preboot Environment to upload**
	  ■ **Netboot**
	  ■ **NetInstall**
	■ **Sysprep Imaging Configuration**

Support for Microsoft Office 365.	PC Transplant now supports Microsoft Office 365.
Support for Thin clients.	Deployment Solution now supports creating images and restoring images on Thin client computers.

What's new in Inventory Solution

The following are the new features for this release:

- New features in Inventory Solution 8.1.
  See Table 1-4 on page 21.
- New features in Inventory Pack for Servers 8.1.
  See Table 1-5 on page 22.

Table 1-4 List of new features in Inventory Solution

Feature	Description
Enhancement in gathering inventory using stand-alone packages. (Windows only)	During standalone inventory, 64-bit stand-alone inventory packages run on the unmanaged 64-bit Windows computers to guarantee more accurate inventory results.

Table 1-4 List of new features in Inventory Solution *(continued)*

Feature	Description
Inventory Solution gathers information for the Symantec Endpoint Protection Windows and Mac clients (SEP) installed in your environment. (Windows and Mac only)	Inventory Solution gathers information for the Symantec Endpoint Protection Windows and Mac clients (SEP) installed in your environment, enabling you to report on the health of the SEP agent. You can view the following information in the **Computers** Management view, in the **SEP Agent** summary flipbook: ■ SEP client name ■ SEP client version and number of devices that have this version installed ■ Number of devices that do not have SEP client installed ■ Number of devices where inventory is not yet gathered To store the gathered SEP data, the new data class **SEP Agent** is introduced on an inventory policy or task page, at **Advanced Options > Data Classes > Software > Common**. This data class is enabled by default based on the type of inventory policy or task. You can view the information for this data class in the **Resource Manager**, by clicking **View > Inventory**, and then selecting the **SEP Agent** data class in the right pane.

Table 1-5 List of new features in Inventory Pack for Servers

Feature	Description
Support for new server applications.	Server Inventory is supported for the following applications: ■ MySQL 5.7.x (not supported for Windows) ■ Microsoft SQL 2016

What's new in ITMS Management Views

In ITMS Management Views 8.1, the following new feature is introduced:

Table 1-6 List of new features

Feature	Description
Symantec Endpoint Protection (SEP) Agent summary flipbook.	You can now see the information about Symantec Endpoint Protection (SEP) Agents that are installed on your client computers. You can view what SEP Agents have out-of-date versions or what client computers do not have SEP Agent installed, or where the SEP Agent inventory data is not current. You can create targets, tasks and policies to solve these issues by using the custom SEP Agent filter criteria. For more information about SEP Agent summary flipbook, please read refer to the following topic in the Symantec Help Center: About the Symantec Endpoint Protection (SEP) Agent summary flipbook.

What's new in Patch Management Solution

In Patch Management Solution 8.1, the following new features are introduced:

Table 1-7 List of new features

Feature	Description
Support for Microsoft Windows 10 feature updates.	Patch Management Solution for Windows supports Microsoft Windows 10 feature updates. For more information about deploying Windows 10 feature updates with Patch Management Solution software update policies, refer to the following KB article: http://www.symantec.com/docs/DOC9422
Support for Microsoft Windows 7/8.1 monthly rollups and security updates.	Patch Management Solution for Windows supports Microsoft Windows 7/8.1 monthly rollups and security updates. For more information, refer to the following article: http://www.symantec.com/docs/HOWTO125807
Support for Microsoft Windows 10 monthly cumulative and delta updates.	Patch Management Solution for Windows supports Microsoft Windows 10 monthly cumulative and delta updates. For more information, see the KB article DOC9705.
Support for Microsoft Office 365 installations that include Office 2016.	Patch Management Solution for Windows supports Microsoft Office 365 installations that include Office 2016 dependent on the availability of the corresponding bulletins in patch data. For more information, see the KB article DOC9673.

Table 1-7 List of new features *(continued)*

Feature	Description
Improved quality and reliability of Red Hat Linux and SUSE Linux computer patching.	Patch Management Solution for Linux 8.1 supports the client-based dependency resolving that offers you the following benefits: ■ More stable and precise ability to resolve dependencies on client Red Hat Linux and SUSE Linux computers. ■ No delays in software update policy creation because dependency resolving is not required at this stage. Only the updates that are selected for distribution are added to a software update policy. ■ Optimization of the network traffic and disk space that is used on Notification Server, package servers, and client computers. During the staging of software bulletins, Patch Management Solution downloads all the updates that are included into the bulletins. However, after the client-based dependency resolving is completed, the additional download occurs only for the dependent software update packages that are required on a specific client computer. For more information about limitations in the client-based dependency resolving, see the KB article DOC9722. For more information about upgrading the Symantec Management Agent and the software update plug-in to 8.1 and applying scheduled software update policies during one Maintenance window, see the KB article DOC9708.
Enhancement in the **Check Software Update Package Integrity** task.	The **Check Software Update Package Integrity** task checks that all software update packages have the correct new settings and values. If some physical files are missing on the file system in the software update package location, this task uses the URL from the latest imported patch metadata to re-download the required files to this location.
Enhanced settings of the software update plug-in. (Windows only)	You can configure the settings that the software update plug-in uses when you install software updates on managed Windows client computers. When you configure the software update installation schedule, you can override maintenance windows settings and let the software update plug-in download required software update packages as soon as a software update policy arrives to the managed Windows client computer. When you choose to notify the user about the restart of the Windows client computer and allow the user to defer the restart, you can benefit from the following options: ■ On the **Default Software Update Plug-in Policy** page, on the **Restart** tab, the option **Remind the user about the restart** lets you set the maximum interval for the notification dialog box to reappear. ■ In the notification dialog box, the user can specify a shorter interval.

Table 1-7 List of new features *(continued)*

Feature	Description
Enhanced options for file download.	Patch Management Solution for Windows supports passive mode FTP and the security protocol TLS 1.2 for file download. For more information on how to enable passive FTP download mode for software update packages, see the KB article INFO3604.
Deprecated platforms.	The following platforms are deprecated in the Patch Management Solution for Linux 8.1 release: ■ Novell SUSE Linux Enterprise Desktop 10 x86/x64 ■ Novell SUSE Linux Enterprise Server 10 x86/x64

What's new in Real-Time System Manager Solution

In the 8.1 release of Real-Time System Manager solution, the following new feature is introduced:

Table 1-8

Feature	Description
KVM Viewer performance improvements.	KVM Viewer is now based on HTML5 and supports various internet browsers including Internet Explorer, Edge Chrome, Mozilla Firefox, Safari and Opera. In the KVM Viewer window you can now see the connection status, messages about last run operation and current client computer power state, host name and IP address. You can now perform various actions directly from the KVM Viewer windows: ■ Activate/deactivate KVM Viewer session ■ Run power options ■ Run CTRL+ALT+DEL action ■ Set image compression and colour mode ■ Set the screen presentation mode either to automatically fit the screen size or show the actual image size For more information, please refer to the following topic in the Symantec Help Center: Running a Keyboard-Video-Mouse (KVM) remote control session.

What's new in Software Management Solution

In Software Management Solution 8.1, the following new features are introduced:

Table 1-9 List of new features

Feature	Description
Reporting of the progress status of a Managed Software Delivery policy.	You can view the progress status of a Managed Software Delivery policy in the Resource Manager, at **View > Inventory > Data classes**, in the data class **Managed Software Delivery Policy Progress Status**. The policy progress status is reported if you check the option **Enable reporting of a policy progress status** in the **Reporting** section. This section is available at the following locations: ■ On the **Managed Delivery Settings** page, on the **Run** tab ■ On the Managed Software Delivery policy page, on the **Policy settings** tab. Note that this option is disabled by default.
Improved usability of the Import Software wizard.	Navigation in the Import Software wizard is improved so that you can easily go back and forth while importing a package to create a software resource.
Removal of Java dependency.	Java Runtime Environment (JRE) is not required for working with Software Catalog and Software Library.
Improved usability of the **Add or Edit Package** dialog box.	When you add a package to a software resource or edit an existing package, you can specify multiple installation files or archive files to a software resource and create custom folders in the target package location. An archive file can be included into the target package content as a single archive file, or it can be extracted into the package contents. The supported archive types for content extraction are ZIP and DMG. When you include an archive file as a single file, the preview of the supported archive file is available.

What's new in User Documentation

The following new format of documentation is introduced:

Table 1-10 List of new features

Feature	Description
Mind maps.	The new format of mind maps is introduced to educate users about different aspects of product usage. Mind maps visualize basic content and the structure of our user guides. For more information and to view the maps, please follow the link: http://www.symantec.com/docs/DOC9706

What's new in Virtual Machine Management

In Virtual Machine Management 8.1, the following new features are introduced:

Table 1-11 List of new features

Feature	Description
Expanded list of supported platforms for Virtual Machine Management	The following operating systems are now supported: ■ CentOS 7 ■ Windows Server 2016

What's new in Workflow Solution

In Workflow Solution 8.1, the following new features are introduced:

Table 1-12 List of new features

Feature	Description
Enhanced ability to design Workflow forms.	Enhanced ability to design forms with the latest Kendo user interface capabilities that AngularJS provides. Added **Show AngularJS Components** check box at the global project to turn on or turn off the AngularJSComponents support.
Enhanced Security.	Enhanced security to support TLS encryption. With this enhancement, new components from Microsoft namespace are used which allow the workflow processes to exchange emails while using TLS encryption
Removed Pervasive.Data.SqlClient.dll from Workflow.	If you are using Pervasive SQL, you must provide a copy of the licensed version of the Pervasive.Data.SqlClient.dll to generate any integration components that need to connect to the Pervasive SQL. For details, refer to the following article: TECH240123

System requirements and supported platforms

Before you install Server Management Suite 8.1, read the **Hardware recommendation** chapter in the *IT Management Suite 8.1 Planning for Implementation Guide* at the following URL:

http://www.symantec.com/docs/DOC9470

For information about the supported operating systems in Symantec Management Platform 8.1 and the Server Management Suite 8.1 solutions, see the *Symantec IT Management Suite Platform Support Matrix* at the following URL:

http://www.symantec.com/docs/HOWTO9965

General installation and upgrade information

Installation of Server Management Suite 8.1

The installation of Server Management Suite 8.1 involves installation of Symantec Management Platform (SMP) 8.1 along with the installation of suites and their solutions using the Symantec Installation Manager.

For more information on how to install and configure the product, see the *IT Management Suite 8.1 Installation and Upgrade Guide* at the following URL:

http://www.symantec.com/docs/DOC9500

Upgrade to Server Management Suite 8.1

You can upgrade from the previous versions of Server Management Suite to the latest version using Symantec Installation Manager.

The following upgrade scenarios are supported:

- From Server Management Suite 7.6 HF7 to Server Management Suite 8.1
- From Server Management Suite 8.0 HF6 to Server Management Suite 8.1

For more information on how to upgrade the product, see the *IT Management Suite 8.1 Installation and Upgrade Guide* at the following URL:

http://www.symantec.com/docs/DOC9500

Migration of Symantec Management Platform and the Server Management Suite solutions

If you want to migrate from older releases where direct upgrade to the latest version is not supported, do the following:

1. Migrate from older release to Server Management Suite 7.5
2. Apply Server Management Suite 7.5 HF6
3. Upgrade to Server Management Suite 7.5 SP1
4. Apply Server Management Suite 7.5 SP1 HF5
5. Upgrade to Server Management Suite 8.0
6. Apply Server Management Suite 8.0 HF6

7. Upgrade to Server Management Suite 8.1

For detailed instructions on migrating to Server Management Suite 7.5, see the following documentation resources:

- *IT Management Suite Migration Guide version 6.x to 7.5* at the following URL: http://www.symantec.com/docs/DOC5668
- *IT Management Suite Migration Guide version 7.0 to 7.5* at the following URL: http://www.symantec.com/docs/DOC5669

For detailed instructions on upgrading from Server Management Suite 7.5 SP1 HF5 to Server Management Suite 8.0, see the following documentation resource:

- *IT Management Suite 8.0 Installation and Upgrade Guide* at the following URL: http://www.symantec.com/docs/DOC8650

Installing Virtual Machine Management

Install the solutions and components in the following sequence:

- Symantec Management Platform
- Deployment Solution
- Symantec Virtual Machine Management

Supported hypervisors

In Virtual Machine Management 8.1, the following hypervisors are supported:

- ESXi 5.0
- ESXi 5.1
- ESXi 5.5
- ESXi 6.0
- Hyper-V (Win 2K8 R2 enterprise)
- Hyper-V (Win 2K8 R2 SP1)
- Hyper-V (Win Server 2012)
- Hyper-V (Win Server 2012 R2)

vCenter 5.0, and vCenter 5.1, vCenter 5.5, and vCenter 6.0 are also supported. They can be used to manage ESXi 5.0, ESXi 5.1, ESXi 5.5, and ESXi 6.0.

Fixed Issues

Server Management Suite 8.1 contains fixed issues for the following solutions and components:

- Symantec Management Platform
  See "Symantec Management Platform Fixed Issues" on page 31.
- Deployment Solution
  See "Deployment Solution Fixed Issues" on page 32.
- Inventory Solution
  See "Inventory Solution Fixed Issues" on page 32.
- Monitor Solution
  See "Monitor Solution Fixed Issues" on page 34.
- Patch Management Solution
  See "Patch Management Solution Fixed Issues" on page 34.
- Software Management Solution
  See "Software Management Solution Fixed Issues" on page 35.
- Virtual Machine Management
  See "Virtual Machine Management Fixed Issues " on page 37.
- Workflow Solution
  See "Workflow Solution Fixed Issues" on page 37.

Note: The issues that were fixed in hot fix releases for ITMS version 8.0 are not included in this document.

For more information about the fixes in hot fix releases, see the following release notes:

- ITMS 8.0 HF1
- ITMS 8.0 HF2
- ITMS 8.0 HF3
- ITMS 8.0 HF4
- ITMS 8.0 HF5
- ITMS 8.0 HF6

Symantec Management Platform Fixed Issues

The following are the fixed issues in this release. If additional information about an issue is available, the issue has a corresponding article link.

The fixed issues are separated into the following components:

- Symantec Installation Manager
  See Table 1-13 on page 31.
- Task Server
  See Table 1-14 on page 31.

Table 1-13 Fixed issues for Symantec Installation Manager

Issue	Article Link
It is not possible to install Migration Wizard 8.0 using Symantec Installation Manager 8.1.	N/A

Table 1-14 Fixed issues for Task Server

Issue	Article Link
Client Task Agent causes GPF (Global Protection Fault) in Symantec Management Agent during the intensive processing of tasks and policies. The agent gets restarted automatically and usually the problem does not re-occur".	N/A

If a task fails by timeout, in the **Task Instance Details** window, the following message appears:
`An unknown exception was thrown.`
When you click the **Show raw exception message** link, the following status appears:
`An unknown exception was thrown.`
`Task was cancelled.`
This issue does not affect any functionality.
	N/A

The following issues have been fixed on the **Tokens** page: ■ Token queries are not saved if the token name contains space. ■ If you click **Cancel** on the **Tokens** page, the SQL statement and the Token name are cleared. ■ Existing token queries do not pass the SQL validation. ■ It is not possible to delete a token or rename a token with an empty name. ■ In token dialog box, the description of the token is not displayed. The **Tokens** page is available in the Symantec Management Console, at **Settings > Notification Server > Task Settings > Tokens**.	N/A

Deployment Solution Fixed Issues

The following are the fixed issues for this release. If additional information about an issue is available, the issue has a corresponding article link.

For more information about the fixes in hot fix releases, see the following release notes:

- ITMS 8.0 HF1
- ITMS 8.0 HF2
- ITMS 8.0 HF3
- ITMS 8.0 HF4
- ITMS 8.0 HF5
- ITMS 8.0 HF6

Table 1-15 Fixed issues for Deployment Solution

Issue	Article link
On a site server, the atrsimg.dll gets installed on the default drive even if the Symantec Management Agent is installed on a non-default drive.	N/A
The PECT agent tries to search nearest Package Server by using the Network Interface Card (NIC) even if the IP address is 169.x.x.x and cannot be routed.	N/A
In case of upgrade, the installation of Deployment Solution Package Server component fails if a few files exist in the PSComponent folder.	N/A
Restore Image task fails to deploy image from a DVD. Following error is displayed: `Image File Selection Error (1909)`	N/A
The Application ID credentials are visible in clear text on the client computers.	N/A
DeployAnywhere fails with an exception while running the **Scripted OS Install** and **Deploy Image** tasks.	N/A

Inventory Solution Fixed Issues

The following are the fixed issues for this release. If additional information about an issue is available, the issue has a corresponding article link.

The fixed issues are separated into the following groups:

- Fixed issues for Inventory Solution
  See Table 1-16 on page 33.

- Fixed issues for Inventory Pack for Servers
  See Table 1-17 on page 33.

Table 1-16 Fixed issues for Inventory Solution

Issue	Article link
Errors related to invalid characters (like `hex 0x1F`) appear in the Notification Server's logs when processing the inventory data collected on Windows computers.	N/A
The file rule **FileName contains *<file name>*** collects no data for the files that match this rule if the file rule **FileType equals *<file type>*** for the corresponding files is not present in the software scan.	N/A
After you install the Inventory Plug-in, you can gather inventory using the options /fi, /dhi, /dswi, /fsi and /dsi of the utility `InvSoln.exe` only after you successfully run the corresponding predefined inventory policy on your client computers.	N/A
The predefined task **NS.Nightly schedule to associate Software component to software product** times out and does not associate software components to appropriate software products.	N/A
When you collect inventory data about active TCP/UDP ports in your environment, the work of Symantec Management Agent is terminated.	N/A
The CPU and processor count data is not collected on the systems HP-UX 11i v3 (PA-RISC and Itanium) with multi-core CPUs.	N/A
In the **Software Product** dialog box, the **Identify inventory** and **Meter / track usage** tabs do not display a software component if at least one target computer reported it as hidden. After the fix, the tabs do not display a software component only if all target computers report it as hidden.	N/A
The custom inventory data classes that are created on the target Notification Server or a child Notification Server are not visible and not available for editing on the **Manage Custom Data Classes** page after replication of the custom data classes from another Notification Server or parent Notification Server.	N/A
The installed date in the **Patch Windows** data class is reported incorrectly.	N/A

Table 1-17 Fixed issues for Inventory Pack for Servers

Issue	Article link
Inventory data for Oracle instances is not reported correctly from the UNIX/Linux Oracle Database servers if the `oratab` files located on a client computer have extra characters at the ends of the lines.	N/A

Table 1-17 Fixed issues for Inventory Pack for Servers *(continued)*

Issue	Article link
Inventory Pack for Servers does not collect information about Oracle Database 12 installed on Windows computers.	N/A

Monitor Solution Fixed Issues

The following are the fixed issues for this release. If additional information about an issue is available, the issue has a corresponding article link.

Table 1-18 Fixed issues for Event Console

Issue	Article link
Event Console Purging Maintenance is not running correctly and as a result "stale" events recur in the Event Console.	N/A
When you use **Performance Counter** metric rules in a policy, the alerts are not auto-resolved from the Event Console.	N/A

Patch Management Solution Fixed Issues

The following are the fixed issues for this release. If additional information about an issue is available, the issue has a corresponding article link.

Table 1-19 Fixed issues for Patch Management Solution

Issue	Article link
When multiple versions of kernel are installed on a Linux computer, the system assessment scan incorrectly reports old kernel versions as applicable in spite of the installed new kernel versions. After the fix, the system assessment scan reports as applicable the versions of kernel that are applicable only to the highest installed version of kernel.	TECH234834
When you add new languages on the **Import Patch Data for Windows** page, the new Microsoft Office 365 language pack updates are not added to the software update policies with Microsoft Office 365 packages, even if you enable the option **Automatically revise Software Update policies after importing patch data**.	N/A
Patch Management Solution fails to download software update packages if it cannot set the security permissions for the downloaded files (for example, on NAS devices).	N/A

Table 1-19 Fixed issues for Patch Management Solution *(continued)*

Issue	Article link
If some language cultures are missing in Configuration Management Database (CMDB), the **Import Patch Data for Windows** task runs successfully but fails to create the associations with the missing languages. As a result, the Patch Remediation Center does not show the software bulletins for the corresponding languages in the list of the bulletins released in the current Patch data release.	TECH236019
When you click **Import channels** on the **Import Patch Data for Red Hat** page to download the list of available software channels, the import of the Red Hat Network (RHN) channels fails because of missing Red Hat certificate chain.	TECH239707

FTP download of software update packages uses active FTP mode only.
To download software update packages in passive FTP mode, use the following registry setting:
`Registry key : HKEY_LOCAL_MACHINE\SOFTWARE\Altiris\Patch Management`
`Registry value [DWORD]:UseFTPPassiveMode`
`Value: 0=OFF(Use Active Mode), 1=ON(Use Passive mode), default value is OFF`
	INFO3604

A software update policy does not download a software update package immediately and stays in pending state until a maintenance window opens.	N/A
The updates for the RealVNC vendor cannot be downloaded due to the SSL error.	N/A

Software Management Solution Fixed Issues

The following are the fixed issues for this release. If additional information about an issue is available, the issue has a corresponding article link.

Table 1-20 Fixed issues for Software Management Solution

Issue	Article link
A blank page is displayed to a user when the Software Portal is loading and looking up for the user membership on the domain and local groups.	N/A
The Restart Manager stops and does not restart the Symantec Management Agent on target Windows computers if a **Managed Software Delivery** policy with custom credentials starts the installation that requires the restart of the Symantec Management Agent.	N/A

Table 1-20 Fixed issues for Software Management Solution *(continued)*

Issue	Article link
Prior to Software Management Solution 8.1, it is not possible to run software delivery tasks as part of client jobs on the computers that have no Software Management Solution plug-in installed or on unmanaged computers. Such computers are excluded from the target during task or job instance creation. After the fix in 8.1, the following changes are introduced: ■ You can run the **Quick Delivery** and **Package delivery** tasks as part of a client job only on the computers without Software Management Solution plug-in. **Note:** Including such a computer to the job target causes the Software Management Solution license consumption for that computer. ■ You can run the **Quick Delivery** and **Package delivery** tasks as part of a client job only and only once on the computers without the Symantec Management Agent (unmanaged computers). For example, you can run these tasks as part of Deployment Solution imaging jobs that install the required agents and plug-ins. **Note:** Including an unmanaged computer to the job target does not cause the Software Management Solution license consumption for that computer. This functionality is not available out of the box and not enabled by default. For more information on how to enable this functionality, see the KB article DOC9717. **Note:** Despite the availability of this functionality, Symantec recommends installing the Symantec Management Agent and Software Management Solution plug-in on every computer where you want to run software management tasks. You cannot run software delivery tasks as standalone tasks on the computers that have no Software Management Solution plug-in installed or on unmanaged computers.	DOC9717
The Software Portal Plug-in Policy with the default filter does not apply to the computers that have an older version of the Software Management Plug-in installed.	N/A
If the user receives a **Managed Software Delivery** policy and postpones it for a period of time, and then, during this time, the administrator disables the policy, the pop-up notification window **New Software is Available** still appears.	N/A
After you disable the **Apply to Resource Targets** and **Enable policy** permissions for a user of a **Managed Software Delivery** policy, the user is still able to modify the targets in this policy and enable or disable the policy.	N/A
After you change the order of dependency tasks in a **Managed Software Delivery** policy and save the changes, the tasks are still sorted in a random order.	N/A

Virtual Machine Management Fixed Issues

The following are the fixed issues for this release. If additional information about an issue is available, the issue has a corresponding article link.

Table 1-21 List of fixed issues

Issue	Article link
The **OS Name** column of **Host Summary Report** does not display the details of the operating system of the ESX server.	N/A
Host resource's description in the Resource Manager data is missing for some hosts.	N/A

Workflow Solution Fixed Issues

The following are the known issues for this release. If additional information about an issue is available, the issue has a corresponding article link.

Table 1-22 Fixed issues for Workflow Solution

Issue	Article link
Codescript Component variable validation does not work.	N/A
Logicbase.Deployment.CreateVirtualDirectory (refactor LogicBase.Components.CreateIIS comps) model is now removed from the Process Manager.	N/A
After you upgrade from Workflow 7.6 to 8.x, an error is displayed if you use a Workflow or process that contains the Code (Script) Component.	TECH239658
Menu select control fails and displays the following error: `Partial selection required`	N/A
The **Update Process Last Modified Date** does not save the UTC time in the database.	N/A
For different time zones, sometimes you can run the tasks immediately and sometimes you cannot work on the tasks for a considerable time.	N/A
The Pause Execution Workflow only considers Anonymous authentication and does not accept Windows and basic authentication.	N/A
For languages other than English, some of the Field names and other details appear in English for the following: ■ In the **My Task List** of the **Process Manager**. ■ In the Symantec Management Console, navigate to **Manage > Workflows > Select Workflow Enterprise Management** and click **Repository > View Versions**.	N/A

Table 1-22 Fixed issues for Workflow Solution *(continued)*

Issue	Article link
For Japanese language, the following text appears in English when you navigate to **Manage > Workflows > Workflow Enterprise Management > Repository > Views** in the Symantec Management Console: `This workflow is what is called by the "Enterprise Management Deployment" plugin from Workflow Designer when a user does not have permission to deploy to a managed Environment.`	N/A
The Terminate Window and Close Dialog option fails to close the dialog box.	N/A

Known Issues

Server Management Suite 8.1 contains known issues for the following solutions and components:

- Symantec Management Platform
  See "Symantec Management Platform Known Issues" on page 39.
- Deployment Solution
  See "Deployment Solution Known Issues" on page 52.
- Inventory Solution
  See "Inventory Solution Known Issues" on page 53.
- ITMS Management Views
  See "ITMS Management Views Known Issues" on page 61.
- Monitor Solution
  See "Monitor Solution Known Issues" on page 62.
- Patch Management Solution
  See "Patch Management Solution Known Issues" on page 65.
- Real-Time System Manager
  See "Real-Time System Manager Known Issues" on page 71.
- Software Management Solution
  See "Software Management Solution Known Issues" on page 76.
- Virtual Machine Management
  See "Virtual Machine Management Known Issues " on page 83.
- Workflow Solution
  See "Workflow Solution Known Issues" on page 83.

Symantec Management Platform Known Issues

The following are the known issues for this release. If additional information about an issue is available, the issue has a corresponding article link.

The known issues are separated into the following components:

- Notification Server
  See Table 1-23 on page 40.
- Task server
  See Table 1-24 on page 41.
- Symantec Management Agent
  See Table 1-25 on page 46.
- UNIX/Linux/Mac
  See Table 1-26 on page 47.
- Network Discovery
  See Table 1-27 on page 49.
- Pluggable Protocol Architecture (PPA)
  See Table 1-28 on page 50.
- ASDK
  See Table 1-29 on page 51.
- ITMS Management Views
  See Table 1-30 on page 51.
- Topology Viewer
  See Table 1-31 on page 51.
- Security Cloud Connector
  See Table 1-32 on page 51.

Table 1-23 Known issues for Notification Server

Issue	Article link
During the upgrade to ITMS 8.1, the custom site server certificate is replaced with the default certificate. **Workaround:** Manually apply the custom site server certificate newly after the upgrade. Take the following steps: 1 In the Symantec Management Console, on the **Settings** menu, click **All Settings**. 2 In the left pane, expand **Notification Server > Site Server Settings**, and then click **Global Site Server Settings**. 3 On the **Global Site Server Settings** page, under **Certificates Rollout**, click the master certificate. 4 In the **Select Certificate** dialog box, click the custom certificate that was applied to the site servers before the upgrade, and then click **OK**.	N/A
When you replicate custom task with custom password from ITMS 7.6 HF7 v10 server to ITMS 8.1 server with FIPS enabled, the replication fails with the following error in the log: "**Unable to decrypt credentials, in case of migration please check that KMS keys were also migrated from old NS.**" **Workaround:** Disable FIPS on ITMS 8.1 server and replicate the required data.	N/A
The upgrade to the latest version of ITMS fails if you configure the IIS settings for the Default Web Site and enable HTTP redirection feature using your Notification Server hostname.	N/A
Setting the value of **VisiblePkgFiles** setting in **CoreSettings** to true and initiating package distribution points update removes the **Hidden** attribute from the files or folders inside the imported packages.	N/A
If you migrate the Configuration Management Database (CMDB) to a different server and then migrate other data with the Migration Wizard, some full licenses that were previously applied are not restored in the new Symantec Management Platform installation. Those are reverted to the trial or the extended trial licenses.	N/A

The aexconfig fails to reset service account if the password contains a ^ character, like in the following example:
`AeXConfig.exe /svcid user:altiris\SRVC_AeXNS_Dev password:pass^w"ord`
`AeXConfig.exe /svcid user:altiris\SRVC_AeXNS_Dev "password:pass^w"ord"`
	N/A

If package server is installed on a computer with host name that contains double byte or HIASCII characters, packages cannot be downloaded.	N/A

Table 1-23 Known issues for Notification Server *(continued)*

Issue	Article link
If you open the **Task Instance Details** window on a parent Notification Server, to check the details of a replicated task, the **Close** option does not let you close this window. This problem occurs because the **Task Instance Details** window is identified as in the Internet zone instead of in the Local intranet zone and the functions of the **Close** option are prevented. To avoid this issue, add the URL of child Notification Server to the list of trusted sites. For more information, read the Microsoft knowledge base article 303650. **Workaround:** Use the **X** symbol in the upper right corner of the window, to close the **Task Instance Details** window.	N/A
Occasionally the **www publishing** service `w3wp.exe` process causes very high CPU and Memory usage. It can cause the computer to stop responding. It is a problem on low-end Windows servers with single core processors. To work around this issue, restart the **www publishing** service.	TECH176493
If you have a hierarchy of Notification Servers, some reports display summary data for each Notification Server. These reports let you drill down into the results. To drill down you click the appropriate row in the results grid for detailed data about a particular Notification Server. However, if a Notification Server is installed to a non-default website and port, its summary data is displayed correctly in the summary report. Any attempt to drill down to display the detailed data fails. A new browser window opens to display the report results, but it contains a Server Error message saying that the resource cannot be found.	N/A
If the Symantec Management Console is set up to use a non-default port, you may see an exception error in the following situation: you try to add computers on the **Agent Push** page of the console by using the FQDN (non-localhost). The following error message is displayed: Data for the page you are currently viewing has expired. **Workaround:** Use the appropriate IP address in the console URL rather than using the FQDN.	N/A

Table 1-24 Known issues for Task Server

Issue	Article link
The information on the right pane of the **Task Version History** dialog box is not displayed properly. Note that this problem appears after installing the Microsoft security update KB4012216.	

Table 1-24 Known issues for Task Server *(continued)*

Issue	Article link
During the upgrade to ITMS 8.1, the following error may appear in the logs: "**Task execution engine failed Could not find stored procedure 'CtsGetMerges'.**" Note that this warning does not cause any functional problems.	N/A
Task Server notifies client computer if a new task is available for it. If there are too many of such notifications, the Symantec Endpoint Protection (SEP) might treat these notifications as port scan attack and block connections from Task Server for 10 minutes. **Workaround:** In SEP, add an allow rule for Task Server so that the SEP does not trigger.	N/A
User-based targets are visible and can be added to the tasks that do not support these targets.	N/A
If you have uninstalled Task Service on your Notification Server and then perform upgrade to IT Management Suite 8.1, the Task Service gets re-installed. To restore the previous state of your Notification Server, you must uninstall the Task Service again after the upgrade.	N/A
In ITMS 8.1, **Anonymous Authentication** is disabled for the **ClientTaskServer** website. That may lead to situation where client computer is not able to access Task Server. For example, if Notification Server and Task Server are in domain and configured under the domain user and the client computer is not in domain. You may need to set up the **Agent Connectivity Credentials** to let the client computers access the **ClientTaskServer** website.	N/A
You cannot install or upgrade Task Server if supported version of .NET Framework is not installed on the computer. One of the .NET Framework versions from 4.5.1 to 4.6 must be installed on the task server computer. Also, note that Windows XP, 2003 Server, and Windows Vista operating systems are not supported for the Task Server install in 8.1.	N/A
Issues with Task Server functionality after repair or upgrade if Task Server is installed on Notification Server.	TECH234031
When you install task server on a Windows 10 computer, multiple errors and warnings appear in windows application log. For example: "**Windows cannot copy file C:\Users\Default\NTUSER.DAT to location C:\Users\Classic .NET AppPool\NTUSER.DAT. This error may be caused by network problems or insufficient security rights**". Note that such errors and warnings are logged only once and do not cause any functional issues for the operating system or for the Task Server functionality.	N/A

Table 1-24 Known issues for Task Server *(continued)*

Issue	Article link
After you upgrade to IT Management Suite 8.0 and enable FIPS, the task that contains encrypted data fails on the clients that are not upgraded to 8.0. If you then disable FIPS, and try to run the same task again on the same clients, the task still fails. **Workaround:** Re-saving the task updates the task version in database and requires the client to re-download the task instead of using the cached task.	N/A

When you upgrade your remote task server, Windows installs multiple updates for Microsoft Framework. Installation of the Framework updates may cause the remote task server to become non-functional and the clients are not able to register to that server.
Workaround: To resolve this issue, run the following command:
`aspnet_regiis.exe /iru`
The `aspnet_regiis.exe` file can be found at one of the following locations:
`%windir%\Microsoft.NET\Framework\v4.0.30319`
`%windir%\Microsoft.NET\Framework64\v4.0.30319` (on a 64-bit computer)
	N/A

After the upgrade, you sometimes cannot select task or policy items in the left pane, and the right pane cannot display the contents of a task or policy. If the content of the task or policy is not loaded in the right pane, the wait sign is displayed or a blank page is loaded. **Workaround:** Open Internet Explorer options and delete **Temporary Internet files and website files**. Reload the Symantec Management Console.	N/A
If you create and run a **Run Script** task that contains incorrect JavaScript syntax, the task fails, but the status of this task is given as **Completed**.	N/A
If you run a Task Server task with the option **Now** or with a custom schedule with disabled **Override Maintenance Window** option, it ignores the active Maintenance Window and runs anyway.	N/A
The Symantec Management Agents that communicate with Notification Server via proxy are not able to connect to the tickle port.	N/A
When you install Symantec Management Agent on a new client computer, the following error message might appear in the logs: `Removed record for not allowed endpoint, because no such endpoint is registered on NS.` This issue does not affect any functionality.	N/A

Table 1-24 Known issues for Task Server *(continued)*

Issue	Article link
The **Run Script** task can be created and saved, but if the syntax is incorrect the task fails. Following error is displayed: `An unknown exception was thrown. System.Data.SqlClient.SqlException: Incorrect syntax near '0'.` **Workaround:** Fix the incorrect syntax of the token. On the **Run Script** page, under **Script Details**, replace the *{0}* with the number of the actual NIC that is used: *1* or *2*.	HOWTO95510
If you create a Control Service State task with the Restart action and you use the full service name, the task fails. **Workaround:** Use the short service name in the task configuration.	N/A
When you install or upgrade task server on a remote client computer, warnings about firewall exceptions can be registered in Notification Server's and Symantec Management Agent's log files. The issue occurs when Windows Firewall service is disabled or stopped.	N/A
When the data is replicated from the parent Notification Server, error messages regarding the performance counter for Task Server can be logged on the child Notification Server. The cause of this issue is the fact that the CTDataLoader service tries to update before they are initialized. This issue does not affect any functionality.	N/A
If you have uninstalled a solution, and there are some custom jobs that contain task using that solution, those jobs cause error messages to appear in the Symantec Management Console. For example, if you create a job with tasks from Patch Management Solution and then remove that solution, in the Symantec Management Console, an error message appears every time you click that job. Additionally, a detailed error message is visible in the Altiris Log Viewer. Jobs with recurring schedule produce an exception in the Altiris Log Viewer every time the schedule is executed. To stop the jobs with recurring schedule from producing errors every time the job is scheduled, do the following: ■ In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**. ■ In the left pane, right-click the task that produces an error, and then click **Properties**. Then, in the **Properties** window, find out what is the task GUID. For example, you can copy it to a text file. ■ On the Notification Server computer, open the Task Scheduler. To do that, you can press Windows + R, and then, in the **Run** dialog box, enter `taskschd.msc`. Then, click **OK**. ■ In the Task Scheduler, in the left pane, click **Task Scheduler Library**. Then, in the right pane, find the task that has the same Guid included in its name and right-click it. Then, click **Delete**.	N/A

Table 1-24 Known issues for Task Server *(continued)*

Issue	Article link
For a task that is executed in hierarchy, if you use **Rerun Failed** on the parent Notification Server, the **Selected Devices** field is not populated with clients reporting to a child Notification Server. This problem occurs because task execution statuses are not replicated from the child Notification Server to the parent Notification Server. **Workaround:** When you use **Rerun Failed** on parent Notification Server, under **Selected Devices**, enter the missing targets manually.	N/A
If you create a task with a schedule on parent Notification Server, the schedule of the task can trigger the replication of this task. In this case, the Windows Task Scheduler on child Notification Server does not display the **Last Run Time** for this task after the task runs. **Workaround:** Replicate the task before its schedule triggers the replication. For example, you can use the **Replicate now** option to replicate the task.	N/A
If you create a **Client Task Schedule** policy and apply it to a revoked or blocked client computer, the scheduled policy is not delivered to this computer and the task does not run. However, on Notification Server, on the **Client Task Schedule** page, the status of this policy is displayed **0% Started** instead of **Failed**.	N/A
In the **Task Instance Details** dialog box, two different data sources are used for the **Start time** value. In the left pane, the **Start time** data is taken from the managed computer. In the right pane, the data for both **Start Time** and **End Time** is taken from the Notification Server computer. The difference appears if the time data between the Notification Server computer and the managed computer is not synchronized.	N/A
The sample client task **Delete Temporary Files** does not delete any files on Windows Vista, 7, 8, 2008, or 2012 operating systems. The task does not delete files on these operating systems for all user profiles because it looks for the files in the wrong location.	TECH160710
The initial use of ".\username" causes any script tasks that are specified as Machinename\username to fail with the error 'Unable to open the file.' This error is due to a profile loading problem. This issue applies only to some operating systems, such as Window XP SP2 and Windows 2003. It does not apply to Windows 7 or to Windows Vista Ultimate SP2.	N/A

Table 1-25 Known issues for Symantec Management Agent

Issue	Article link
The Symantec Management Agent 7.6 HF7 fails to register on Notification Server 8.1, after receiving the following settings from the Notification Server 7.6 HF7: ■ **Agent Communication Profile** that has Cloud-enabled Management settings specified. This profile is exported from Notification Server 8.1 and imported to Notification Server 7.6 HF7. ■ Custom **Targeted Agent Settings** policy that has the option **Specify an alternate URL for the Symantec Management Agent to use to access the NS** enabled and communication profile imported from Notification Server 8.1 specified, and also the option **Allow Windows agent to perform Cloud-Enabled registration on specified Notification Server** enabled. This issue occurs only if the Notification Server 8.1 is running on Windows 2012 R2 Server. **Workaround:** On Notification Server 8.1, add registry DWORD **"ClientAuthTrustMode"=dword:00000002** at the following location: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL]	N/A
In some cases, TLS 1.2 connection might not work between Symantec Management Agent and Notification Server. This issue was introduced by Microsoft and has been fixed now. Make sure that you get the latest updates for your Microsoft Windows Server 2012 R2.	N/A
Client computers that are installed from Cloud-enabled Management offline packages are not part of the default **Cloud-enabled Management Settings** policy targets and don't receive the changes in the default **Cloud-enabled Management Settings** policy. **Workaround:** Clone the **Cloud-enabled Management Settings** policy, and then manually add targets based on the CEM Agents installed from package `pkg_name` filter.	N/A
For Symantec Management Agent to start, permissions for SYSTEM user on `C:\Users\All Users\Microsoft\Crypto\` folder and its contents should be set to **Allow**. If those permissions are set to **Deny**, Symantec Management Agent does not start, and the following error message is logged: `Failed to initialize agent storage: Access is denied (0x00000005)`	N/A

Table 1-25 Known issues for Symantec Management Agent *(continued)*

Issue	Article link
In some cases, Windows XP and Server 2003 computers with Symantec Management Agent installed may show a delay on boot, at the Applying computer settings screen. The cause of this issue is Symantec Management Agent's startup type being set to **Automatic**. **Workaround:** Change the Symantec Management Agent service startup type to **Manual**.	TECH211289
On client computers with Internet Explorer 10 installed, Symantec Management Agent help might not be properly formatted. For example, images are not displayed.	HOWTO95650
If you have revoked the Symantec Management Agent of a package server, it can take up to three hours before clients assigned to that package server can download packages from Notification Server.	N/A
When you perform a push installation of Symantec Management Agent to a computer that has McAfee All Access 2012 installed, the installation fails.	N/A

Table 1-26 Known issues for UNIX/Linux/Mac

Issue	Article link
After performing an off-box upgrade of IT Management Suite from version 7.6 to 8.0 it is not possible to redirect the 7.6 CEM agents on OSX computers to communicate with 8.0 Notification Server in CEM mode. **Workaround 1:** Take the following steps: 1 Ensure that the 7.6 agents are able to communicate with the 8.0 Notification Server without using CEM. 2 On 7.6 Notification Server, disable the CEM policy to remove the old CEM settings from the agents and configure the **Targeted Agents Settings** to redirect the agents to 8.0 Notification Server.. 3 On the 8.0 Notification Server, enable the CEM policy. After the 7.6 agent registers on 8.0 Notification Server and receives the CEM policy, it receives the new CEM settings. **Workaround 2:** Re-install the agent using the Cloud-enabled Agent installation package.	N/A
Due to file system limitations, Package Server running on Linux-based operating system does not support more than 30000 packages for ext3 file system and not more 65000 for ext4 file system, leading to unavailability of packages in case the number of packages exceeds this limitation.	N/A

Table 1-26 Known issues for UNIX/Linux/Mac *(continued)*

Issue	Article link
Mac OS X agent does not support the **Run As** options for the Managed Software Delivery policy and the Quick Delivery task. If you change the default **Run As** option from **Symantec Management Agent credential** to **Current logged-on user** or **Specific user**, the Managed Software Delivery policy or Quick Delivery task fails to run on your Mac client computer. This issue appears only when you install native packages in Silent or Interactive mode.	N/A

A custom command metric with the following command line returns an incorrect value on SLES 10:
 	
`ps -ef | grep -v 'grep' | grep -c -i -w "chssrvInfoServerapp01mgtNode01Cell"`
 	
The value that is returned when executed within the OS shell is "1," but the metric returns a value of "0." This value is to monitor if a process is running, but something interferes with the command execution of the metric. The cause is a character limitation of 32 characters of the desired process name (not a character limitation of the entire command-line syntax).
 	
The command returns either a "1" or a "0"; therefore, the character length of the process name should not be an issue, but it is.
 	
If you configure the command line of the metric as follows, it returns the correct value:
 	
`ps -ef | grep -v 'grep' | grep -c -i -w "chssrvInfoServerapp01mgtNode01Ce"`
 	
Note: This issue does not appear to exist on RHEL computers.
	N/A

You cannot enable a package server password for Linux Package Server when **Publish HTTP codebase** is enabled. A certain security risk exists if you disable anonymous access to a Linux package server in HTTP mode. Linux package servers support only "basic authentication". Consequently, passwords are sent in plain text. Use either HTTPS or keep anonymous HTTP access for a Linux package server.	N/A
Known limitations exist on supported Apache configurations for the computer that is intended as a package server candidate. For example, HttpdIntegration does not properly parse Apache config file with SSL and custom. Please avoid using complex Apache configurations on such computers.	N/A
After you make a time zone change on a UNIX/Linux/Mac client, the change may not affect running services until after you restart the client system.	N/A

Table 1-26 Known issues for UNIX/Linux/Mac *(continued)*

Issue	Article link
The AIX `inittab` service does not support any of the actions that are available in the **Service Action** drop-down list. When the AIX `inittab` service is checked, the **Service Action** field should be grayed out and not selectable. At present this field is (incorrectly) functional in the Symantec Management Console. To avoid errors in your Service Control task, set the **Service Action** field to **No action**. This action prevents any attempt to execute Start, Stop, Restart, or Get Status commands for AIX `inittab` services. Note that currently the No action setting is incorrectly processed and cannot be used for task creation. As a result, all Service Control tasks that are created for the `inittab` service control system are reported as failed. The error message “Missing or invalid service action” is displayed. This message appears regardless of whether the specified process or service was successfully modified.	N/A
Some basic inventory information, such as Time zone, OS language, Primary User, and host id, may not be reported for certain ULM systems (Solaris, HP-UX, and RedHat).	N/A

Table 1-27 Known issues in Network Discovery

Issue	Article link
When you perform Network Discovery using SNMP protocol, the incorrect operating system is shown for Windows 10, and for Windows Server 2016 computers. For Windows 10, Windows 8.1 is displayed. For Windows Server 2016, Windows Server 2012 is displayed.	N/A
When Network Discovery for Windows Embedded Standard 7 SP1 client computers is performed using WMI Connection profile and credentials, the results are displayed as Microsoft Windows Embedded Standard 6.1 65 instead of Windows Embedded Standard 7 SP1.	N/A
Discovery tasks do not identify duplicate identity values among discovered devices. While you run a discovery task, virtual machines with the same UUID are considered as one device. Accordingly, one CMDB resource is created for those devices.	N/A
When running the hierarchy differential replication schedule in certain upgrade scenarios, you may get exceptions such as: "Incompatible columns in DataClassAttribute. Error:Class Name: VM Guest" in the Notification Server computer log. Break the hierarchy before upgrading. Then, upgrade both parent and children before re-joining.	TECH154203

Table 1-27 Known issues in Network Discovery *(continued)*

Issue	Article link
In the Symantec Management Console, when you enter into **Maximum number of threads per discovery task** field different value than 1-99, a warning message is displayed. Regardless of the Symantec Management Console language, that warning message is always in English.	N/A
In the Symantec Management Console, on the **Network Discovery** portal page, in the **Network Discovery Task Management** Web Part, on the **Task runs** tab, there is a stop icon that becomes active even when no tasks are selected.	N/A

Table 1-28 Known issues in Pluggable Protocol Architecture (PPA)

Issue	Article link
PPA plug-in requires .NET 4.5.1 to function properly, but .NET 4.5.1 installation is not supported on Windows 2003 computer. If you try to install PPA plug-in on a Windows 2003 computer, the installation fails.	N/A
After the server restart, the `AtrsHost` service might stop responding with an exception that references to PPA_x64. The root cause of this issue is incorrect practice of using the connection profiles. When the connection profile has some protocols enabled without credentials or when credentials are there but they are not selected, the service stops responding. **Workaround:** Create proper credentials for the connection profile, select them, and then enable the appropriate protocol.	N/A
Remote Monitoring Server (RMS) of Monitor Solution stops responding on computer having Windows Server 2012/2012 R2 and .NET Framework 4.0. .NET Framework 2.0 is a prerequisite for the Pluggable Protocol Architecture (PPA) agent installation. When you enable .NET Framework 3.5 from the **Add Roles and Features** wizard, .NET Framework 2.0 gets installed automatically. .NET Framework 2.0 does not get installed automatically on installing .NET Framework 4.0. Because .NET Framework 2.0 is not installed on the computer, the PPA agent installation is affected, which in turn affects RMS. **Workaround:** Enable .NET Framework 4.5.1 on the computer and then install PPA.	N/A
WMI, WSMAN, and other monitoring plug-ins become unavailable if multiple web-service identities are used. You must ensure that you remove multiple identities if you choose a custom website.	TECH142631

Table 1-29 Known issues in ASDK

Issue	Article link
To use the `ExecuteTask` ASDK method, you have to be a member of the Symantec Administrators security role.	N/A
SecurityManagement.AddRolePrivileges and SecurityManagement.RemoveRolePrivileges do not work on right-click privileges. An automated workaround using the ASDK currently does not exist. However, right-click privileges can be added to a role and removed from a role using the Symantec Management Platform item update process.	N/A
ItemManagement.SetItemsSchedule does not successfully set a schedule on a policy item. Currently a workaround using the ASDK does not exist.	N/A

Table 1-30 Known issues in ITMS Management Views

Issue	Article link
When you navigate from the **Manage** menu to **Computers**, **Software**, **Policies**, or **Jobs/Tasks**, the section doesn't open if the name of Notification Server that you are connecting to contains non-alphanumeric characters.	N/A

Table 1-31 Known issues in Topology Viewer

Issue	Article link
During the upgrade from ITMS 8.0 to 8.1, the language pack for Topology Viewer is not installed. **Workaround:** Manually install the language pack after the upgrade in the Symantec Installation Manager, on the **Optional Installations** page.	N/A

Table 1-32 Known issues in Security Cloud Connector

Issue	Article link
When you import device data from Unified Endpoint Protection to the child Notification Server, the imported devices are replicated up to parent Notification Server. However, the organizational views and groups in which these devices reside, are not replicated up to parent. As a result, the imported devices only appear under the default **Computer** organizational group.	N/A
Not all user data that is imported from Unified Endpoint Protection to the child Notification Server, is replicated up to the parent Notification Server. Only device owners are replicated up.	N/A

Table 1-32 Known issues in Security Cloud Connector *(continued)*

Issue	Article link
The resources that are imported from Unified Endpoint Protection to Notification Server are not purged on Notification Server.	N/A

Deployment Solution Known Issues

The following are the known issues for this release. If additional information about an issue is available, the issue has a corresponding article link.

Table 1-33 Known issues for Deployment Solution

Issue	Article Link
Deployment Solution fails to import SysPrep Image with Resource Import Tool on package server.	N/A
Symantec Management Server Error page is displayed when you try to access **Settings > Deployment** page.	N/A
PC Transplant and imaging tasks fail, if the Primary file storage location is configured in the package server **Settings** page.	N/A
Extract SSL certificate fails when Notification Server is installed with non-Default website.	N/A
Import Computers option of the **Predefined Computers** page does not open when when the **Respond to Predefined computers** is checked on the **NBS General Settings** page.	N/A
After you deploy an RHEL 7.2 XFS file system image using multicast on virtual client computer, the **Boot to Production** task fails. Workaround: Manually restart the computer.	N/A
The **Copy file** task fails to copy files or folders using the UNC path when FIPS mode is enabled on a Linux client computer. Workaround: Disable the FIPS mode and run the task again.	N/A
The **Boot To** task fails to boot a Mac client computer as the System Integrity Protection feature is introduced in Mac OS X 10.11. Workaround: Run the csrutil disable command in the Recovery Mode.	N/A

Table 1-33 Known issues for Deployment Solution *(continued)*

Issue	Article Link
You can launch the Resource Import Tool only with a Service Account.	N/A
You cannot install the Network Boot Service on a Windows 8.1 computer as the Network File System (NFS) service is not listed in a Windows 8.1 computer.	N/A
A UEFI-based computer with secure boot mode enabled is unable to boot to production when deploying a BIOS-based Windows 8 64-bit image.	N/A
The NFS shared path is not enabled for the MacNetShare folder, even when the NFS service is installed for a Windows Server 2008 SP2 NBS computer.	N/A

Automation folder is not installed on a Mac 10.10 computer.
Workaround:
Run the following command on all CoreStorage enabled disk on a Mac OS X 10.10 computer when booted in the production environment:
`diskutil coreStorage revert <diskidentifier>`
For example:
`diskutil coreStorage revert disk1`
	N/A

After replication of preboot configurations (automation folder and PXE) from parent Notification server to child Notification Server, only the version of the default WinPE is displayed on the **Manage Preboot configurations** page of the child Notification Server. Workaround: Recreate all the preboot configurations from the **Manage Preboot configurations** dialog of the child Notification Server with the desired WinPE version.	N/A
On replication, custom drivers as well as their tags that are added from the parent Notification Server are not visible on the **Driver Management** dialog of the child Notification Server.	N/A

Inventory Solution Known Issues

The following are the known issues for this release. If additional information about an issue is available, the issue has a corresponding article link.

The known issues are separated into the following groups:

- Installation and upgrade issues.
  See Table 1-34 on page 54.
- Hierarchy and replication issues.
  See Table 1-35 on page 54.

- Other known issues that are common for all types of platforms.
  See Table 1-36 on page 54.
- Other known issues for Windows platforms.
  See Table 1-37 on page 55.
- Other known issues for UNIX, Linux, and Mac platforms.
  See Table 1-38 on page 56.
- Known issues for Inventory Pack for Servers.
  See Table 1-39 on page 57.

Table 1-34 Installation and upgrade issues

Issue	Article link
After you upgrade the Symantec Management Agent to the latest version, the old version Inventory Plug-in may experience troubles collecting some data. To avoid this problem, you should always upgrade Inventory plug-in to the latest version.	N/A

Table 1-35 Hierarchy and replication issues

Issue	Article link
If the parent Notification Server and child Notification Server have different region time format settings, the **Days Metered** count on the **Underutilized Software** report page displays incorrect value.	N/A
When you replicate an inventory task from a parent Notification Server to a child Notification Server in a hierarchy, you can edit the advanced options of the replicated task on the child NS computer. After you edit the advanced options of the replicated task on the child NS computer and click **Save changes**, the changes that you made are not saved. Normally, the advanced settings on the replicated task page should not be editable, and the Save changes and Cancel options should not be enabled.	N/A

Table 1-36 Other known issues that are common for all types of platforms

Issue	Article link
Inventory scan does not report the information about file language when you enable the option **File properties - manufacturer, version, size, internal name, etc.** on an inventory policy or task page.	N/A
Inventory reports display incorrect **Install Date** for installed software products.	N/A

Table 1-36 Other known issues that are common for all types of platforms *(continued)*

Issue	Article link
During full inventory scan, file inventory is not collected for the software components that are not .MSI based. You cannot view file inventory data when you right-click a non-MSI based software component, click **Actions > Edit Software Resource**, and then click the **File Inventory** tab. As a result, you cannot automatically meter the usage of this software component as it has no file inventory and is not associated with an executable file. To enable a non-MSI based software component for metering, you should manually add executable files to the software component.	N/A
A license is not reclaimed when the **Asset Status** is set to a custom asset status. Inventory Solution or Inventory Pack for Servers license should be reclaimed on setting the **Asset Status** to other than **Active**.	N/A

Table 1-37 Other known issues for Windows platforms

Issue	Article link
Inventory scan does not report the amount of Video RAM larger than 4GB because of limitations of the Microsoft methods that the scan currently uses for collecting Video Controller information.	N/A
SCDP Inventory task and software scan may overwrite the contents of the table dbo.Inv_InstalledSoftware with their own different results.	N/A
Software Catalog Data Provider Inventory task may incorrectly detect several languages of the same software component as several components that are installed on the same client computer.	N/A
An inventory policy that runs under the **System account** does not collect inventory information about Network Printers. To collect this information, you need to run the policy as a **Logged in user**.	TECH145268
When you use Internet Explorer 10 or 11 to download a stand-alone package, an error occurs. This issue occurs because of the **SmartScreen Filter** security feature by Microsoft. You can directly download the package exe from the `NSCap` folder on the server, and run it on unmanaged client computers.	N/A

Table 1-37 Other known issues for Windows platforms *(continued)*

Issue	Article link
After the NS.Nightly schedule task runs, the Yahoo! Messenger is displayed in the Software Catalog under **Newly Discovered Software** instead of under **Unmanaged Software**.	N/A
When you configure the advanced options for the Inventory policy and include a file scanning rule for a file type that is not in a default list, the files are not scanned if the file type is written in capital letters.	N/A
If you run a standalone inventory package on a managed client computer with installed NS Agent and the inventory execution is terminated unexpectedly, the NS Agent may be left in nonfunctional state. To resolve this issue, you need to register the original NS Agent .dlls manually using the following command lines: Regsvr32 "C:\Program Files\Altiris\Altiris Agent\AeXBasicInventory.dll" Regsvr32 "C:\Program Files\Altiris\Altiris Agent\Agents\SoftwareManagement\"SMFAgent.dll" Regsvr32 "C:\Program Files\Common Files\Altiris\AeXNetComms.dll" Regsvr32 "C:\Program Files\Common Files\Altiris\ AeXNSEvent.dll"	N/A

Table 1-38 Other known issues for UNIX, Linux, and Mac platforms

Issue	Article link
Errors related to invalid characters (like `hex 0x1F`) appear in the Notification Server's logs when processing the inventory data collected on UNIX, Linux, or Mac computers.	N/A
Inventory scan does not report Model ID for some Mac client computers.	N/A
Running three software inventory tasks simultaneously on UNIX, Linux, and Mac computers results in the system overload and long execution time because CPU usage increases to 100%. As a workaround, you can schedule the tasks to avoid running them simultaneously.	N/A
After you run some inventory task with delta inventory enabled on one Notification Server computer, redirect Inventory Plug-in to another Notification Server computer, and run another inventory task with delta inventory enabled along with some other types of inventory, only delta inventory data is sent.	N/A
Inventory scan does not scan deeper than maximum length paths limitation.	N/A
HW_DiskPartition data class cannot be populated on AIX platforms.	N/A

Table 1-39 Known issues for Inventory Pack for Servers

Issue	Article link
When you upgrade the 7.x Inventory Pack for Servers Plug-in to 8.1, inventory task configuration files for the following predefined server inventory policies are removed from the `InvTaskConfig` folder: ■ **Collect Full Server Inventory** ■ **Collect Delta Server Inventory** In such case, you can gather server inventory using `InvSoln.exe/fsi` or `InvSoln.exe/dsi` only after you successfully run the predefined server inventory policies on your client computers.	N/A
The data classes that are related to Oracle Database information and require Oracle credentials are populated only when the Inventory Pack for Servers Plug-in has the same version as the Inventory Plug-in.	N/A
A stand-alone package cannot be created after Inventory Pack for Servers has been uninstalled.	N/A
When you view the data class information in the Resource Manager, on the **IIS Settings** page, the values for some fields are not populated. This happens because Microsoft IIS version 8.0 drops some registry keys and Inventory Solution cannot report inventory for these fields.	N/A
Server inventory cannot be collected on a 32-bit MS SQL server that is installed on a 64-bit OS.	N/A
During Server inventory, a warning **Failed to execute WMI query** appears in the Agent log if Network Load Balancing is not installed.	N/A
Full inventory for Microsoft SQL Server 2012 is not gathered when you run an inventory policy or task using the advanced option **System account**.	N/A
An inventory task with the disabled MySQL data class but with valid MySQL credentials it collects MySQL data on Linux computers.	N/A
An Inventory policy or task that runs with the root rights when collecting the inventory on SUSE Linux Enterprise Server or on AIX cannot log into the Oracle database. This problem does not occur on Red Hat Enterprise Linux, Solaris, and HP-UX Oracle servers. As a workaround, you can create an inventory policy or task that collects inventory for Oracle data classes only and runs with non-root user credentials.	N/A

Table 1-39 Known issues for Inventory Pack for Servers *(continued)*

Issue	Article link
Inventory Pack for Servers tries to inventory the data classes for various supported server components, such as Microsoft Exchange Server, Microsoft IIS Server, and so on, irrespective of whether server components are present. This does not result in slowing down the inventory process. However, some traces, like “Could not collect the inventory information for xxxx”, “Failed to collect inventory for xxxx”, “Execution of query Failed”, or “Failed to inventory information from WMI. Error: … ” are added to the log files when you run an inventory task for gathering server data classes with the **Enable verbose client logging** option selected at **Advanced option > Run Options**.	N/A
The **DHCP Scopes** and **DHCP Options** data classes incorrectly report the values that have double quotes.	N/A
The reported version of the DHCP server does not match with the DHCP version given in the **About** dialog of the DHCP server.	N/A

Table 1-39 Known issues for Inventory Pack for Servers *(continued)*

Issue	Article link
With IIS 7.0 installed on Microsoft Windows Server 2008, some fields of the following IIS data classes are not populated correctly, even if the Management Compatibility features are installed. Fields of **IIS Http VirtualDir Setting Data** data class: ■ Content Location ■ Default Document Enabled ■ Default Document Name ■ Script Source Access Enabled ■ Access Read Enabled ■ Access Write Enabled ■ Directory Browsing Enabled ■ SSL Access Enabled ■ Content Expiration Enabled ■ Content Expiration Setting ■ Log Enabled ■ Execute Permission Fields of **IIS Http Host Setting Data** data class: ■ Content Location ■ Default Document Enabled ■ Default Document Name ■ Script Source Access Enabled ■ Access Read Enabled ■ Access Write Enabled ■ Directory Browsing Enabled ■ SSL Access Enabled ■ Content Expiration Enabled ■ Content Expiration Setting ■ Log Enabled ■ Execute Permission Fields of **IIS Http Server Setting Data** data class: ■ Central Binary Logging Enabled ■ Rapid Fail Protection Interval ■ Rapid Fail Protection Max Crashes	N/A

Table 1-39 Known issues for Inventory Pack for Servers *(continued)*

Issue	Article link
On a freshly installed operating system, before executing a server inventory stand-alone package or a server inventory task for gathering Microsoft Exchange Server data classes, you must explicitly install the Microsoft Visual C++ 2005 SP1 Redistributable Package (x86). Otherwise, the inventory for the data class **Exchange Mailboxes** is not gathered. The Microsoft Visual C++ 2005 SP1 Redistributable Package (x86) installs run-time components of Visual C++ Libraries that are required to run the applications that use these run-time components. Server Inventory Plug-in depends upon these libraries and run-time components. You can download the package for free at http://www.microsoft.com/downloads/details.aspx?familyid=200b2fd9-ae1a-4a14-984d-389c36f85647&displaylang=en	N/A
On Windows Server 2003 operating system, inventory of the **Exchange Mailboxes** data class is only populated when you use “Logged In” user context. On Windows 2000 Server operating system, inventory of the **Exchange Mailboxes** data class is not populated. Inventory for Microsoft Exchange Server 2007 is not supported. Exchange Inventory does not return data from Exchange Server Clusters.	TECH47438
The **License Type** and **Number of License** fields are not populated in the **SQL Server License** data class.	N/A
Inventory Pack for Servers Plug-in for Windows does not implement the logic for populating the following fields: ■ The **Block Size** field of the **Oracle Database** data class. ■ The **Block Size** and **File System Size** fields of the **Database Storage Area** data class for Oracle 9i. ■ The **Users High Watermark** field of the **Oracle Database Service** data class.	N/A
MySQL details for the **DB_Database Service** data class are not populated when MySQL service is stopped. Inventory of installations of multiple instances of MySQL Server on a computer is not supported. If multiple instances are installed, the inventory is gathered for the first instance that is found.	N/A

Table 1-39 Known issues for Inventory Pack for Servers *(continued)*

Issue	Article link
If you select any kind of database inventory (for example, Oracle, MySQL or MS SQL) from the data class tree view, Inventory gathers data for almost all the databases (Oracle, MySQL, and MS SQL) installed, irrespective of selection in the tree view because most of the data classes are common among them. If you disconnect from the registered server running SQL Server through SQL Server Enterprise Manager by right-clicking the server name and clicking the **Disconnect** menu, then, after gathering the inventory, the **Operational Status** property of the **Database Service** data class is not reported.	N/A
Only a single instance of Apache Server is supported for Inventory. (Windows only) If the value for the **KeepAliveTimeout** parameter is specified in the configuration file `httpd.conf` of Apache web server, then after gathering the inventory, NSE loading fails for the data class **Http Host Setting Data** on Notification Server.	N/A

ITMS Management Views Known Issues

The following are the known issues for this release. If additional information about an issue is available, the issue has a corresponding article link

Table 1-40 Known issues for ITMS Management Views

Issue	Article link
You can select **Hardware Summary** and **Operating System Summary** data classes in the Custom Criteria dialog box if the root Data Classes have been disabled for your particular user role.	N/A
A target cannot be saved to an empty root directory.	N/A
If the version of the installed Server Inventory plug-in is earlier than 7.6, the expected plug-in version is displayed as N/A.	N/A
You may experience problems when downloading ITMS Management Views. In this case, Symantec recommends that you clear the browser cache.	N/A
When you navigate from the **Manage** menu to **Computers**, **Software**, **Policies** or **Jobs/Tasks**, the corresponding section doesn't open if the host name of Notification Server that you are connecting to contains underscore characters. To resolve this issue, you need to change the server host name or connect to the server using the IP address.	Domain names Session variables

Monitor Solution Known Issues

The following are the known issues for this release. If additional information about an issue is available, the issue has a corresponding article link.

The known issues are separated into the following groups:

- Monitor Solution
  See Table 1-41 on page 62.
- Event Console
  See Table 1-42 on page 65.

Table 1-41 Known issues for Monitor Solution

Issue	Article Link
Monitor service fails to install with an error during the configuration of Remote Monitoring Server. Workaround: To resolve the issue, Install Microsoft .NET Framework 4.5.1 on the target server, then rollout Symantec Management Agent and Windows Remote Monitoring Plugin and then install Monitor service.	N/A
During the upgrade, Symantec Installation Manager displays the following components as partially installed: • Altiris Monitor pack for servers languages • Altiris Monitor solution pack for servers languages Workaround: To resolve the issue run the following command from the command prompt: **Msiexec /i "C:\Program Files\Altiris\Symantec Installation Manager\Installs\Altiris\altiris_monitorpackserverslanguages_7_6_x64.msi" /qb SKIPAIM=1**	N/A
In some cases, monitored resource that is managed in CEM mode is available as a target for **Reset Monitored Resource** task. This situation appears if you run the task using **Quick Run** or **New Schedule** run options.	N/A
After you add and save a new rule and then send alerts based on the rule, the categories Hostname, Definition, and Protocol are not displayed correctly on the Management Station console.	N/A
Customized **Monitor Plug-in rollout** policy targets are rewritten with default values during upgrade.	N/A
A heartbeat alert may be raised in Event Console from a monitored resource that runs on a virtual machine, even if it is online and the metric provider is running.	N/A

Table 1-41 Known issues for Monitor Solution *(continued)*

Issue	Article Link
Monitor token values that include double quotes cause **VBScript** tasks to fail.	TECH154599
The **Disk Paging Activity** report displays incomplete HP-UX and AIX data when it is viewed in the Chart View.	N/A
Agentless monitoring uses Pluggable Protocol Architecture (PPA) connection profiles.	N/A
On the **Manage Connection Profile** page, when you create connection profiles for different configured clients, the user is not able to assign (to map) connection profiles to the resources.	N/A
WS-Management service cannot process the request on Windows clients.	N/A
Time drifting issues occur when monitoring heartbeats on Linux computers that are hosted on VMware.	N/A
The Poll Metric on Demand task cannot poll agent-based metrics on a computer that does not have the Monitor Plug-in.	N/A
Network Discovery found devices may not be listed in the targeted filters of the default agentless policy. **Note:** The operating system version is correctly discovered for the target computers that have SNMP enabled.	N/A
A failed heartbeat may not raise an alert in the Event Console due to network latency when you have the following configuration: ■ The **Retry every** option on the **Heartbeat** tab of the **Monitor Server Settings** page has a value of "0". ■ The value of the **Check for heartbeats every** option is less than or equal to the **Send heartbeat every** option on the **Data Collection** tab of the **Monitor Plug-in Configuration Settings** page. In this case, a Monitor Plug-in may appear to occasionally go down only to come right back up again. However, the uptime data is not affected in this case.	N/A
Agentless monitoring is not available for the targets that have been discovered through an Active Directory Import. Workaround: Use a Network Discovery or a WINS import instead of an Active Directory Import.	N/A
You must reconnect the Real-time Performance Viewer if metric data becomes unavailable.	N/A

Table 1-41 Known issues for Monitor Solution *(continued)*

Issue	Article Link
Computers are not populated in the Computers List for the Real-time Viewer and Historical Performance Viewer until data is received from the target computer by Notification Server.	N/A
When **Altiris** log type is selected, the Log Event metric only supports Windows platforms.	N/A
HTTP metrics do not support virtual hosts.	N/A
WMI metrics read the data with the lowest polling interval.	N/A
If you add the **Poll metric on demand** task to a policy or to a rule, the task fails to run when the rule is activated. The task completes successfully when manually executed.	N/A
Manually created Monitor site servers disappear after disaster recovery. Workaround: Create Monitor site servers again, manually.	N/A
SQL metric default connection data must be provided to configure **All Windows Servers** policy.	N/A
Log Event metric for FTP log file with **Unlimited file size** setting produces incorrect results. Workaround: Set a constant file size (for example, 64K) for the FTP log file, instead of *unlimited*, when configuring **Log Event** metric.	N/A
Aggregation can only evaluate metrics if they monitor an equal number of instances.	N/A
Policies may get overwritten when creating multiple policies in a new window or from the Server Management Suite portal. Workaround: To get back the overwritten policies, re-import the rewritten monitor packs manually. All monitor pack settings will also be reset to default in this case.	N/A

Table 1-42 Known issues for Event Console

Issue	Article Link
It is not possible to export and import **Alert Rule Settings** from the **Event Console** page. Workaround: On a source server, do the following: ■ In the Symantec Management Console, on the **Settings** menu, click **Monitoring and Alerting**. ■ In the left pane, expand **Event Console**, and click **Alert Rule Settings**. ■ In the right pane, right-click each rule, and then click **Export**. ■ Save the rules. On a target server, do the following: ■ In the Symantec Management Console, on the **Settings** menu, click **Monitoring and Alerting**. ■ In the left pane, expand **Event Console**, and click **Alert Rule Settings**. ■ In the right pane, right-click on any item in the list, and then click **Import**. ■ Select the previously saved rules.	N/A
When you select multiple alerts holding down the Shift key, the **Acknowledge** and **Resolve** options on the toolbar become unavailable. Workaround: Right-click any of the selected items and click **Acknowledge** or **Resolve**.	N/A
In the **Event Console**, the **Select Filter** text box has a limitation. The DBCS input is not supported from neither a physical keyboard, nor using the IME virtual keyboard. Workaround: You can copy DBSC text and paste it into the **Select Filter** text box.	N/A
Internet Explorer error message **about:blank** pops up: **Content from the website listed below is being blocked by the Internet Explorer Enhanced Security Configuration.** Workaround: **about:blank** needs to be added into the **Trusted sites** list of the Internet Explorer.	N/A

Patch Management Solution Known Issues

The following are the known issues for this release. If additional information about an issue is available, the issue has a corresponding article link.

The known issues are separated into the following groups:

- Patch Management for Windows hierarchy and replication issues
  See Table 1-43 on page 66.
- Patch Management for Windows software updates installation issues
  See Table 1-44 on page 66.
- Patch Management for Windows other known issues
  See Table 1-45 on page 68.
- Patch Management for Mac known issues
  See Table 1-46 on page 70.
- Patch Management for Linux installation and upgrade issues
  See Table 1-47 on page 70.
- Patch Management for Linux hierarchy and replication issues
  See Table 1-48 on page 70.
- Patch Management for Linux other known issues
  See Table 1-49 on page 71.

Table 1-43 Patch Management for Windows hierarchy and replication issues

Issue	Article link
After an upgrade from the previous version for which you had to break the existing hierarchy, you need to run **Patch Management Import Data Replication for Windows** once with **Replication Mode = Complete** to ensure that items deleted on parent server are also properly deleted on the child servers (for example, Patch Data bulletins).	N/A
If you run complete replication but do not replicate the patch data, and then try to run the **Vulnerability Scan** task on a child server or a client computer from the Parent Notification Server, the scan fails.	N/A
Replicated policies get deleted on the child Notification Server, when Patch Management Import Data for Windows uses the **Standard Replication Schedule**.	TECH210370

Table 1-44 Patch Management for Windows software updates installation issues

Issue	Article link
A box that you uncheck on page 1 in the **Distribute Software Updates** wizard does not stay unchecked when you switch to the page 2. Workaround: In the Symantec Management Console, on the **Manage** menu, click **Policies**. Create a software update policy, configure, and then enable it.	N/A
Some updates do not support silent installation. Some dialog or progress windows may be visible to the user of the client computer.	N/A

Table 1-44 Patch Management for Windows software updates installation issues *(continued)*

Issue	Article link
Some updates may fail to install in certain conditions. The following updates are known to have issues: ■ Flash Player All Mozilla Firefox browser windows and all instances of Flash Player must be closed before installation. Symantec recommends that you update Flash Player 7.x, 8.x, and 9.x to the latest version. ■ Real Player Installation may fail if a limited user is logged in to the system. ■ Mozilla Firefox version 1.5, 2.0 and 3.0 All Mozilla Firefox browser windows must be closed before installation. ■ Opera Silent installation may fail on Windows XP. ■ Adobe Reader version 7 and 8 All instances of Adobe Reader, including those opened inside of a browser, must be closed before installing updates. Symantec recommends that you install Adobe Reader updates shortly after a computer restart. ■ ISA Server 2000 Security Patch for Web Proxy Service and H.323 ASN DLL (MS01-045) Installation of this hot fix requires user interaction on the target computer. The user must click **Yes** in the installation dialog box.	HOWTO54657
Some software updates are shown as not installed in the **Windows Update** dialog box. This issue occurs because the executable is a full software release, not a patch. Symantec recommends that you use Altiris Software Management Solution from Symantec to roll out this software. The following software updates are known to have this issue: ■ KB982671 - Microsoft .NET Framework 4 ■ KB968930 - Windows PowerShell 2.0 and WinRM 2.0 ■ KB940157 - Windows Search 4.0 IE8 - Internet Explorer 8 ■ KB2526954 - Microsoft Silverlight IE9 - Internet Explorer 9 ■ KB2463332 - Windows Internal Database Service Pack 4	N/A

Table 1-44 Patch Management for Windows software updates installation issues *(continued)*

Issue	Article link
Some updates may require original installation media. The updates that are known to require one are as follows: ■ Microsoft Project 2003 SP3 ■ Microsoft Visio 2003 SP3 ■ Citrix Presentation Server If the product was installed from a CD/DVD, then the original CD/DVD must be inserted in the disk reader on the client computer.	N/A
Issues occur when various Microsoft Office components are having different Service Pack versions applied.	N/A
A removed vendor or software update is displayed in the **Vendors and Software** list. The removed vendor or software release will disappear from the list after the **Import Patch Data for Windows** task is completed.	N/A
The **Windows Computers with Software Update Plug-in** counter works only for the client computers that have the Software Update plug-in originally rolled out from the same Notification Server.	N/A
If you change the package location from default to **Alternative Location** with custom credentials and then back to default, you will not be able to perform **Vendors and Software** update. To complete the update, you need to select **Default Location** and complete the **Vendors and Software** update. You can then switch back to the **Alternative Location**.	N/A
When you deploy Microsoft updates through Patch Management with the restart settings disabled, the operating system still forces the client computers to restart.	N/A

Table 1-45 Patch Management for Windows other known issues

Issue	Article link
An issue when using FTP as patch data alternative download location. If you want to use an FTP location as the alternative download location on the **Import Patch Data** page, on the Notification Server computer, add the `C:\Program Files\Altiris\Notification Server\Bin\AeXsvc.exe` service to the firewall Exception List.	N/A

Table 1-45 Patch Management for Windows other known issues *(continued)*

Issue	Article link
A non-administrator cannot navigate to the AexPatchUtil.exe utility using the command prompt because of access restrictions to the `C:\Program Files\Altiris` folder. This issue occurs only on the Notification Server computer. Workaround: `cd` straight to the `C:\Program Files\Altiris\Altiris Agent\Agents` directory.	N/A
An issue occurs when you re-image or reinstall an operating system on a client computer. Software update plug-in cannot process the policies and install software updates. Workaround: Restart the Symantec Management Agent service or restart the computer.	N/A
Patching of software that is installed into a virtual layer is not supported.	N/A
Packages are not always downloaded to managed computers at the correct time. This is due to a timing issue where the initial download is not triggered by Software Management and the status of the package is not updated. The packages will be downloaded when the update install schedule fires or when the next maintenance window opens.	N/A
When you click **Save Changes** in a policy, a confirmation message displays *Saved Changes* even though the policy is still being saved.	N/A
The Software Update Plug-in stays in the *Update Pending* state after the **Software Update Installation** dialog box closes.	N/A
The **Software Bulletin Details** report shows the computers that are out of the scope of the current console user.	N/A
If you change the settings of the **Advertisement Set** policy, and then run the Patch Management with the **Revise** option enabled, the modified update will not be re-downloaded.	N/A
The out-of-scope client computers are displayed in the **Compliance Summary** report.	N/A
When, on the **Import Patch Data for Windows** page, under **Package Location**, you select **Alternative Location**, you need to enter it in the following format: **<alternative location>/pmimport.cab** Otherwise, if you enter the path in the wrong format, the new location will still be saved successfully, but, the import will fail.	N/A
After the disaster recovery, you need to rerun the Patch Management import.	N/A

Table 1-46 Patch Management for Mac known issues

Issue	Article link
The Mac Software Update Helper Tool might not detect some firmware updates for Mac computers. Therefore, those updates do not appear in the **Available Mac Software Updates** report. Workaround: Manually download the update from the Apple Downloads site. If you are unsure whether your computer needs a particular update, download and open the update installer. The installer indicates whether the firmware update is already installed or is not needed.	N/A

Table 1-47 Patch Management for Linux installation and upgrade issues

Issue	Article Link
On the client computers that have the software update plug-in less then 8.1 installed, the **Linux System Assessment Scan** does not report as applicable the Linux updates with the following characteristics: ■ The updates obsolete another installed update packages. ■ The updates have been imported by the **MetaData Import Task** running on the 8.1 Notification Server. As soon as the software update plug-in on the client computers is upgraded to 8.1, the **Linux System Assessment Scan** reports such updates as applicable.	N/A
Software Update Plug-in 8.1 on Linux clients may be not functional with the state **Waiting for repository** if the task **Import Patch Data for Novel/Red Hat** is not executed after the upgrade to 8.1.	N/A

Table 1-48 Patch Management for Linux hierarchy and replication issues

Issue	Article Link
Exporting software update policies from parent to child is not supported.	N/A
Replicating data between different versions of Patch Management Solution is not supported.	N/A

Table 1-49 Patch Management for Linux other known issues

Issue	Article Link
A user who belongs to the **Patch Management Administrators** role cannot edit default targets in the following policies: ■ Novell patch management configuration policy You access this policy from **Settings > Software > Patch Management > SuSE Settings > SuSE**. ■ Red Hat patch management configuration policy You access this policy from **Settings > Software > Patch Management > Red Hat Settings > Red Hat**. Workaround: On the configuration policy's page, delete the default targets, and then add the appropriate custom targets.	N/A
Task details do not show the cause of the **Import Patch Data for Red Hat** or the **Import Patch Data for Novell** that fail due to lack of free space on the Notification Server computer.	N/A
The **Novell/Red Hat Compliance by Update** report can show an incorrect number of computers on which updates have been installed.	N/A
A software update policy may fail to save. This issue may occur when anonymous access is enabled for the Altiris folder in IIS.	N/A
Automation policy report **Maintain Retired Machine Historical Data** does not return any results.	N/A
Patch Management for Linux uses Linux native tools Yum and Zypper to resolve and install dependent software update packages. On Linux client computers, a software update policy attempts to install in a single transaction all the software updates that are included into the policy and their resolved dependent packages. If the native tool fails to install at least one of the packages, the policy fails to install the other packages too.	N/A

Real-Time System Manager Known Issues

The following are the known issues for this release. If additional information about an issue is available, the issue has a corresponding article link.

The known issues are separated into the following groups:

- SOL/IDE-R issues
  See Table 1-50 on page 72.
- RTCI known issues
  See Table 1-51 on page 73.

- Other known issues
  See Table 1-52 on page 74.

Table 1-50 Known issues for SOL/IDE-R

Issue	Article link
SOL terminal window does not support double-byte characters (Japanese, Chinese).	N/A
The following options must be configured in the ME BIOS advanced settings for Intel AMT Serial-over-LAN to work correctly with HP computers: ■ SOL Terminal Emulation Mode: ANSI ■ Disabled echo char: ON	N/A
When the SOL/IDE-R session is used to remotely boot a Dell client computer from a physical floppy diskette that is inserted into a floppy drive on the Notification Server computer, or from a binary floppy image file, the client computer performs a restart but does not load the operating system. On the client computer's monitor, the message `Attempting remote IDE boot` appears, but the Real-Time System Manager's terminal window remains blank until the session is terminated. This is a known issue with Dell computers (tested on Dell OptiPlex 745c). Workaround: Start the client from other media (physical CD-ROM, DVD-ROM, or ISO image file).	N/A
If a SOL session window is already opened for a computer, you must close it before establishing a new remote SOL connection to the computer. Otherwise, following error message may appear: `SOL session terminated`.	N/A
When SOL and IDE-R are disabled in the target computer's BIOS, the controls for these options on the **Intel AMT Settings** page (**Task progress window and remote control** and **Redirect to optical/floppy drive or image on a server**) are not disabled.	N/A
IDE-R session to an MS-DOS boot image may not work correctly with the managed HP client computers that have BIOS versions earlier than 1.5. Workaround: Upgrade BIOS on the client computer.	N/A
When you use any Alt+<key> sequence on the keyboard during the Serial-over-LAN session, the controlled computer may not receive it.	N/A

Table 1-50 Known issues for SOL/IDE-R *(continued)*

Issue	Article link
Due to SOL emulation limitations, installation of a graphical operating system through IDE-R can lead to a BSOD on some Intel vPro implementations and is not fully supported by Intel AMT 2.x products. The problem affects HP Compaq Business Desktop System BIOS for Intel vPro Technology (786E1 BIOS). Workaround: Download and install the latest BIOS/firmware update from the vendor's website.	N/A
When you establish a SOL/IDE-R session with HP computers with Intel AMT 2.5, the first line of the terminal output is not displayed in the remote console.	N/A
Ctrl+Alt+Del key sequence does not work in the SOL session established with Intel AMT 2.5 devices.	N/A
Function keys do not work in the SOL session. Use use the <Esc>+1 - <Esc>+0 key sequence to emulate the function keys.	N/A
On some hardware (HP, Fujitsu), the SOL/IDE-R session initiated by wireless connection terminates after 1 minute. This is a hardware limitation. To work around this issue, do the following: 1 In the Notification Server computer's registry, set the following DWORD value to *1*: *HKEY_LOCAL_MACHINE\SOFTWARE\Altiris\eXpress\Notification Server\ProductInstallation\ {13987439-8929-48d2-aa30-ef4bf0eb26a6}\InstantAMTPing*. 2 Restart the IIS.	N/A
One-to-many server IDE-R task fails if the IDE-R session is left active from the one-to-one real-time task and vice versa.	N/A
Boot redirection options are not available for DASH computers.	N/A

Table 1-51 Known issues for RTCI/RTSM

Issue	Article link
If the redirection privileges are disabled, it is impossible to execute one-to-one power actions, such as power off or restart.	N/A
It is not possible to run one-to-many out-of-band tasks on IPMI computers. That is because the IP address of the IPMI management controller differs from the computers's IP address. Notification Server does not know the IPMI controller's IP.	N/A

Table 1-51 Known issues for RTCI/RTSM *(continued)*

Issue	Article link
The **Restore State** power action is not capable of putting computers into Stand-by (S3) or Hibernate (S4) states. Consequently, the **Restore State** power action turns off the computer (if needed) in an attempt to restore the Hibernate (S4) state and turns on the computer (if needed) to restore the Stand-by (S3) state.	N/A
The following Intel AMT inventory is not collected by the **Get Out-of-Band Inventory** task: ■ RTCI AMT Battery Serial Number ■ RTCI AMT Battery Manufacture Date	N/A

Table 1-52 Other known issues

Issue	Article link
Error while performing power management operation `Reboot` command. This problem is known for Dell Precision T3500 computers.	N/A
It is not possible to connect to Intel AMT 5.0 using secure WS-MAN connection. To solve this problem, you need to upgrade the Intel AMT 5.0 firmware to the latest Intel AMT 5.2.	N/A
You cannot connect to Intel DASH computer configured in mutual authentication mode.	N/A
IDE redirection does not work with "Kerberos" user.	N/A
Firewall settings prevent WMI connection to a computer running Windows XP Service Pack 2. If you provided valid WMI credentials, but cannot establish a WMI connection to a computer that is running Windows XP Service Pack 2 (WMI is not in the list of supported protocols on the Real-Time Consoles page), check the firewall settings on the target computer. The default configuration of the Windows Firewall program in Windows XP SP2 blocks incoming network traffic on Transmission Control Protocol (TCP) port 445. Configure the firewall to allow incoming network traffic on TCP port 445.	N/A

Table 1-52 Other known issues *(continued)*

Issue	Article link
When using Real-Time System Manager to remotely connect to Windows Vista, Windows 7, Windows 8, or Windows 8.1 client computers, you must make sure that Windows Firewall is configured to allow remote Windows Management Instrumentation (WMI) connections on the client computer. To enable WMI connections on Windows Vista, in the Control Panel, click **Windows Firewall > Change Settings > Exceptions**, and then check **Windows Management Instrumentation (WMI)**. Additionally, for standalone WWindows Vista, Windows 7, Windows 8, or Windows 8.1 clients (not in a domain), you must disable the User Account Control (UAC). For example, to do this for Windows Vista, in the Control Panel click **User Accounts > Turn User account control on or off** and then uncheck **Use User Account Control (UAC) to help protect your computer**. Optionally, you can disable the UAC for the built-in administrator account (if you want to use this account for remote connection). To do this, in the **Control Panel > Administrative Tools > Local Security Policy** MMC snap-in, click **Local Policies > Security Options** and disable the **User Account Control: Admin Approval mode for Built-in Administrator account** policy.	N/A
Connection capabilities limited when connecting to computers that have multiple network cards.	N/A
One-to-many tasks cannot manage resources by an IP address.	N/A
Some Intel ASF hardware does not support power off from the S3 state. You can try to turn on the computer and then run the turn off command again. Broadcom ASF does not have this problem.	N/A
PXE Boot does not work with some ASF hardware.	N/A
Both one-to-one and one-to-many tasks in the Real-Time System Manager software require a direct connection to the target computer that you want to manage. It is not possible to manage computers located behind NAT-enabled routers.	N/A
Graceful shutdown or restart returns an error on Microsoft Windows Vista, Windows 7, Windows 8, or Windows 8.1.	N/A
It is not possible to update properties on the **Operating System** page in the **Real-Time** view if the target computer is running Microsoft Windows Vista (32-bit and 64-bit editions).	N/A
Intel AMT computer management using CIRA is possible only with Intel AMT 4.0 and later computers that are configured to use TLS or TLS with mutual authentication.	N/A
It is impossible to connect to Intel DASH computer configured in mutual authentication mode.	N/A

Table 1-52 Other known issues *(continued)*

Issue	Article link
In the **Real-Time** view, on the **Intel AMT Configuration Mode** page, the setup and Configuration Server address is not shown for computers with Intel AMT version 2.6 and 4.0.	N/A
During upgrade, custom configuration of Network Filtering resets to default. To keep using the custom setting you need to do the following: ■ On your NS Server, from the *\RTSM\Web\UIData* folder, copy the `CBFilters.bak` file. ■ Rename the `CBFilters.bak` file to `CBFilters.xml`. ■ Replace the original xml with the one containing the custom configuration.	N/A
The trace route doesn't work from the **Real-Time System Manager Portal** page. To work around this issue, in the Symantec management Console, right-click the selected resource, and then, in the right-click menu, click **Remote Management >Trace Route**.	N/A
It is not possible to connect to a remote computer using local account. Whether you are connecting to a remote computer in a domain or in a workgroup determines whether User Account Control (UAC) filtering occurs. In a workgroup, the account connecting to the remote computer is a local user on that computer. Even if the account is in the Administrators group, UAC filtering means that a script runs as a standard user. Workaround: A best practice is to create a dedicated local user group or user account on the target computer specifically for remote connections.	https://msdn.microsoft.com/

Software Management Solution Known Issues

The following are the known issues for this release. If additional information about an issue is available, the issue has a corresponding article link.

The known issues are separated into the following groups:

- Installation and upgrade issues
  See Table 1-53 on page 77.
- Managed software delivery issues
  See Table 1-54 on page 78.
- Software Portal issues
  See Table 1-55 on page 80.
- Hierarchy and replication issues

See Table 1-56 on page 80.

- Non-Windows-specific issues
  See Table 1-57 on page 81.
- Software Management Framework issues
  See Table 1-58 on page 81.
- Other issues
  See Table 1-59 on page 82.

Table 1-53 Installation and upgrade issues

Issue	Article link
A Managed Software Delivery policy with the compliance schedule window, which is set for a time period in the past, re-executes after the on-box upgrade from ITMS 7.5 SP1 HF5 to ITMS 8.0 and the upgrade of Symantec Management Agent and Software Management Solution Plug-in on the client computer.	N/A
If you import custom software resources to `\\<NS>\NSCAP` UNC share, and then upgrade Symantec Management Platform, the software is removed during the process.	N/A
After upgrade from IT Management Suite 7.0, previous versions of Symantec Management Agent and Software Management Plug-in may fail to run Managed Delivery Policies and Quick Delivery tasks under specific user credentials. Workaround: Upgrade Symantec Management Agent and Software Management Plug-in or run Managed Delivery Policies and Quick Delivery tasks using Symantec Management Agent credentials.	N/A
Managed Software Delivery policies stay in the detection check state after upgrade. If Managed Software Delivery policies stay in the detection check state on the client computer for a long time after upgrade, then they may not get executed. Workaround: To fix this issue, restart the affected client computer or the corresponding Symantec Management Agent.	N/A
Modified installation error code descriptions are reset to default values, after upgrading from Software Management Solution 7.0.	N/A
Migrated software components are not merged with newly discovered software components if those components have separate 32-bit and 64-bit versions. After upgrading to Software Management Solution 7.5, software component duplicates appear in Software Catalog, after running Software Discovery for those components which have 32-bit and 64-bit separate versions.	N/A

Table 1-53 Installation and upgrade issues *(continued)*

Issue	Article link
Custom policies for Symantec Workspace Virtualization, Software Streaming or Virtual Composer stop working after upgrade. Initiate package distribution point update to resolve the issue. Display of an updated version of Symantec Workspace Virtualization, Symantec Workspace Streaming or Virtual Composer is displayed in **Software Releases** requires a manual update.	N/A
If you enable Legacy Agent Communication mode after you upgrade Notification Server, the "Windows computers with installed Software Management plug-in" filter along with the tasks and policies, based on this filter does not work, unless the Software Management plug-in is up-to-date.	N/A
The version of the Virtual Composer in the software resource package remains unchanged, after upgrading to the latest version of Software Management Solution. Detection and applicability rules, based on the Virtual Composer version must be updated manually.	N/A
Software Virtualization related resource items for deleted packages appear in the Software Component Type Organizational Group, after upgrade to the latest version of Software Management Solution.	N/A
If you have custom Managed Delivery policies, Quick Delivery tasks or Package delivery tasks, which use Symantec Workspace Virtualization Agent, you have to manually recreate such tasks or policies after upgrade to the latest version of Software Management Solution.	N/A
If the Software Library is inaccessible during the upgrade to the latest version of Software Management Solution, software packages are not grouped properly on the IIS web server.	N/A

Table 1-54 Managed software delivery issues

Issue	Article link
You can create a Managed Software Delivery policy and schedule compliance or remediation to start running at computer startup. If the policy is received approximately 20 minutes after the target computer startup, the policy runs as soon as the computer receives the policy.	N/A
When you schedule many Managed Software Delivery policies, and on the **Managed Delivery Settings** page, in the **Actions after success** section, select the advanced option **Log off user**, the other policies in the queue are postponed until the post-execution restart of the client computer occurs.	N/A

Table 1-54 Managed software delivery issues *(continued)*

Issue	Article link
When you schedule a Managed Software Delivery policy and on the **Managed Delivery Settings** page, in the **Run As** section, select the advanced option **Symantec Management Agent credential** or **Current logged-on user**, and then in the **Task can run** section, select the advanced option **Only when user is logged on**, the policy does not respect the selected settings and runs at the scheduled time, even if the user is not logged on a client computer.	N/A
After you run a Managed Software Delivery policy on a managed client computer, SMA restart occurs during the policy execution, and then you cancel the software installation, the last status **Success** is incorrectly displayed for **Execute install command** on the client computer, on the **Symantec Management Agent** toolbar, in the **Software Delivery** tab. At the same time, the policy is correctly reported as not compliant on the client computer and in reports on Notification Server.	N/A
Managed Software Delivery policy may fail to install a software application into a virtual layer on computers running Windows 7 Embedded operating system.	N/A
If Managed Software Delivery policy is created for a software, which has a dependency on another software, using **Managed Software Delivery** wizard, where on the **Specify dependencies and updates** page the **Verify dependencies** option is checked and the software resource option is unchecked for the corresponding software, the dependent software is not installed even if the dependency option is later checked in the policy settings. Workaround: To fix the issue, remove the software resource from the Managed Software Delivery policy and add it again.	N/A
Managed Software Delivery policy or a Quick Delivery task fail to run from a directory on the Notification Server computer with a 1619 error code, if the following conditions are met: ■ Managed Software Delivery policies and Quick Delivery tasks fail to run from a directory on the Notification Server computer. ■ There are no package servers in an environment; ■ A software resource is imported from a Notification Server; ■ The **Use the following settings to download and run** option is checked; ■ The **Download and run locally if bandwidth is above** is unchecked; ■ The **Run from server if bandwidth is above any connection speed** is checked; ■ The **Current logged-in user** option is checked on the **Run Options** settings.	N/A

Table 1-54 Managed software delivery issues *(continued)*

Issue	Article link
When running a Managed Software Delivery policy under **Currently logged in user**, the file version detection check fails to detect a file, which is located under the %user name% folder. Workaround: To fix the issue, in the file location path, use the %useprofile% environment variable, which points to the same folder.	N/A
When running a Managed Software Delivery policy under **Currently logged in user**, the **Registry Key/File Path to File Version** and the **Registry Key/File Path to Product Version** detection rules fail to detect a file, if the path is specified using environment variables.	N/A
If multiple users log in locally or remotely to the client computer, on which a software resource is installed by a Managed Software Delivery Policy, and specify different settings, when prompted to restart the computer after the software installation is complete, the following situations may occur: ■ If a client computer user snoozes the computer restart, after a software resource is installed by a Managed Software Delivery policy, computer can only restart, when this user is logged in again. If another user logs in to the same client computer and selects to restart the computer after the installation is complete, the computer does not restart. ■ If a user has accepted computer restart, but it was snoozed by another user, or the maintenance window has not started yet, the computer will then restart unexpectedly for the first user, when the snooze period, specified by another user expires or the maintenance windows starts.	N/A

Table 1-55 Software Portal issues

Issue	Article link
When migrating from Software Management Solution 6.x, the Software Portal publishing permissions for a software resource change their status from **Approved** to **Requesting Approval**.	N/A

Table 1-56 Hierarchy and replication issues

Issue	Article link
When you run **Differential Hierarchy update** from the Parent Notification Server to the Child Notification Server, a Managed Software Delivery policy gets replicated every differential replication, if you enable the option **Power on computers if necessary (using Wake-on-LAN, Intel AMT, ASF or DASH)** on the **Managed Delivery Settings** page or under the **Schedule** section that appears when you create or edit the policy.	N/A

Table 1-57 Non-Windows-specific issues

Issue	Article link
A false-positive status for a software package on a Mac client computer may be reported, if the user cancels the software interactive installation. If a user of a Mac client computer cancels a Quick Delivery task or a Managed Delivery task, which has an interactive install, the success execution event is sent to the Notification Server, leading to a false-positive status for this installation. At the same time, the software scan for the Quick Delivery task and the detection check for the Managed Delivery task provides the correct information.	N/A

Table 1-58 Software Management Framework issues

Issue	Article link
If you import computer resource information from an XML file, exported from another Notification Server, the computer resource information related to installed software in the Resource Manager is lost.	N/A
Source Path Update and Windows Installer Repair tasks fail with error code - 1073741515 on computers, running Windows Server 2012 R2 Core operating system.	N/A
The **Log off user** option in the **Managed Software Delivery** policy logs off only a single session rather than all sessions when multiple sessions are active. For more information, see topics on Results-based actions settings in Software Management Solution in the *IT Management Suite Administration Guide* at the following URL: http://www.symantec.com/docs/DOC7978 Workaround: Use the **Log off** option available with the **Restart Computer** task to successfully log off every session.	N/A
Files in the **File Inventory** tab are overwritten if a software resource is moved to **Managed Software** and metering is turned on for this software resource.	N/A
If you create a Quick Delivery task and the task times out before the maintenance window is activated on the client, the task fails. By default, a task times out after 300 minutes. On the **Task options** tab of the Advanced settings, you can change when a task ends.	N/A
With a Managed Software Delivery policy or Quick Delivery task, applications with large installation paths fail to execute.	TECH133459
When creating a package by ASDK **AutoGenerateCommandLines** parameter set to **True**, no command lines are generated for the package.	N/A

Table 1-58 Software Management Framework issues *(continued)*

Issue	Article link
If you add one large file or a very big number of small files, estimating around 2 GB in total, the procedure will fail with errors in the Notification Server computer log file, while editing a software resource.	N/A
Setting weak ACL, such as "Everyone", for a shared location, which is used for the Software Library, may lead to intentional or unintentional loss of Software Library data or lack of storage on the corresponding server. Workaround: To prevent the issues, set strong ACL for UNC path, which leads to the Software Library repository.	N/A
When importing software packages using Import Software wizard, package files can be read by an unauthorized party during data transfer from package store to the Notification Server computer. If package files contain sensitive information, such as passwords inside scripts, in unencrypted form, then such software import can be a subject to information disclosure threat.	N/A

Table 1-59 Other issues

Issue	Article link
Detection rules do not detect the registry key **Binary Value** while determining whether a specific instance of a software application is installed on a client computer.	N/A
Symantec Workspace Virtualization Agent uninstallation task may fail with an error due to restart of Symantec Management Agent and Task Agent. The task will be completed after the restart of Symantec Management Agent.	N/A
Applicability rule for a software resource does not work, when re-importing the software resource using the Replicator tool on a different Notification Server, after the initial rule is changed.	N/A
Unable to generate a command line for a package from a Software Library. If the Software Library is specified as a source for a package containing large files, while editing an existing software resource, the command lines are not generated for this software resource.	N/A
Software discovery creates second software resource for a software resource that is imported from MSI. If after running the Software Discovery task or gathering software inventory, Software Catalog duplicates previously imported software resources as newly discovered software resources, this means, that the corresponding imported MSI files contained different software keys. Workaround: To fix the issue, run the Merge Duplicate Resources scheduled task. If this task does not fix all issues, merge the software resources manually.	N/A

Table 1-59 Other issues *(continued)*

Issue	Article link
You must restart the client computer after you uninstall the Symantec Workspace Virtualization Agent from it using the "Uninstall SWV agents" policy. Otherwise, the software applications, installed into virtual layers may stop working correctly.	N/A
If you run a Detailed Export for a software resource, which has a "conflicts with" association, then this association is not displayed after importing the resource from the XML file.	N/A
An error appears, when trying to install Wise Toolkit on a server with installed Software Management Solution 7.5 as a result of the end-of-life of Wise Package Studio.	TECH210284

Virtual Machine Management Known Issues

The following are the known issues for this release. If additional information about an issue is available, the issue has a corresponding article link.

Table 1-60 List of known issues

Issue	Article link
Virtual Machine Management does not support creation of a Guest OS with the new computers that have Mac OS X 10.12, but supports upgrade of the existing computers that have Mac OS X 10.10 or earlier.	N/A
In the **Resource Manager**, the **VM Discovery** task displays incorrect description details for the VM name.	N/A
In the Virtual Machine Management page, the following details of the guest virtual machines are not displayed on HYPER-V hypervisor: ■ CPU utilization ■ Memory utilization	N/A

Workflow Solution Known Issues

The following are the known issues for this release. If additional information about an issue is available, the issue has a corresponding article link.

Table 1-61 Known issues for Workflow Solution

Issue	Article link
Workflow Service stops after upgrade from 8.0.HF6 to 8.1.	N/A

Table 1-61 Known issues for Workflow Solution *(continued)*

Issue	Article link
Microsoft Edge Reading view is not supported. Use the normal mode to view Process Manager and Workflow pages	N/A
Access denied error is displayed while opening project packages containing some DLL files that were created in the earlier build. Workflow Solution fails to copy or create the DLL files in the customlib directory. Workaround: For the logged in user, manually grant access to the Symantec install directory.	N/A
If the base URL contains hostname, the published web form does not open in the Microsoft Edge browser. Workaround: Open the URL in Internet Explorer 11 or use that fully qualified hostname, IP address, or localhost in the base URL.	N/A
After an off-box upgrade to Symantec Management Platform 8.1, the older projects cannot be republished from Workflow Designer. This is because the default **Local SMP** environment has information about the older SMP server. Workaround: To resolve this issue, delete the old SMP server from SMP, manually register the new Workflow Server, and add the new server to the **Local SMP** environment. Republish the project from Workflow Designer.	N/A
After an off-box upgrade to Process Manager 8.1, the existing AD synchronization might not run because the background server in the Process Manager master setting has information about the older Process Manager server. Workaround Delete the old background server and manually add the new server to the background server from the Process Manager settings and then restart IIS.	N/A
For languages other than English, some fields on the following pages of the Project Manager appear in English: ■ **Add Email Template** ■ **Add Rule** ■ **Master Setting** ■ **Workflow Task Details**	N/A
For languages other than English, some fields on the Home page of the **Process Manager portal** appear in English.	

Other things to know about Server Management Suite 8.1 solutions and components

- Symantec Management Platform
  See "Other things to know about Symantec Management Platform" on page 85.
- Inventory Solution
- Monitor Solution
  See "Other things to know about Monitor Solution" on page 89.
- Patch Management Solution
  See "Other things to know about Patch Management Solution" on page 89.
- Software Management Solution
  See "Other things to know about Software Management Solution" on page 90.

Other things to know about Symantec Management Platform

The following are the things to know about this release. If additional information is available, the information has a corresponding article link.

Things to know are separated into the following components:

- Notification Server
  See Table 1-62 on page 86.
- Task server
  See Table 1-63 on page 87.
- UNIX/Linux/Mac
  See Table 1-64 on page 87.
- Network Discovery
  See Table 1-65 on page 88.
- Data Connector
  See Table 1-66 on page 89.
- SymHelp
  See Table 1-67 on page 89.

Table 1-62 Things to know about Notification Server

Information	Article link
When you perform an off-box upgrade, the FQDN of the old server and the new server differs. To maintain the connectivity of the agents after the upgrade, Notification Server automatically updates the default communication profile of the old server with the FQDN of the new server. After this change, the communication profile of the old server will remain available, but all references to it are switched to the communication profile of the new server. The agent settings that point to the custom communication profile are not changed during the upgrade process.	N/A
Default times for differential replication and for the **NS.Daily** schedule do not allow to perform Differential or Complete replications within the same night. Default **NS.Daily** schedule, which collects summary data is set to run every day at 02:10 AM. By default, the differential replication is set to run every day at 01:00 AM, Complete replication runs at 2:00 AM. This means that the summary data for a given day is replicated on the next day. To replicate the summary data on the same day it is collected, change the time for the **NS.Daily** schedule to run before the replication starts.	N/A
In hierarchy, the **Source** field in **Resource Manager** always indicates Notification Server from which the client computer was replicated. Server field is used to indicate Notification Server that the client computer reports to.	N/A
The package server uses ACLs to restrict access to the folders and files that it owns. Installation of the package server on a file system without ACLs implementation is supported, but not recommended. The following file systems do not include the ACL functionality: ■ UFS ■ FAT ■ VFAT ■ FAT32	N/A
If you attempt to upgrade across collations, the database reconfiguration fails with the following error message: Cannot resolve the collation conflict. The database and the database server collations must match. This function is by design: Symantec Management Platform does not support upgrading across different collations.	N/A
The user name for the Symantec Management Agent ACC cannot include any special characters	N/A

Table 1-63 Things to know about Task Server

Information	Article Link
If you replicate a task with **system** attribute from parent Notification Server to its child and run this task on a child Notification Server's client computer, the task will not run and its status will be marked as **Failed**.	N/A
When you create a **Client Task Schedule** policy on parent Notification Server and replicate it to a child Notification Server, the schedule of this policy is not always displayed on the **Client Task Schedule** policy page of the child Notification Server. The schedule of the policy is only displayed, when you open the default view of the **Client Task Schedule** policy page. After you make changes under **Policy Status**, in the **View** drop-down list, the schedule of the policy disappears. However, the policy runs successfully by schedule.	N/A
If a computer is in a workgroup environment then some tasks (for example **Delete Temporary Files**) advanced settings require the user name in full format, *computer_name\user_name*.	N/A
Installation of a Task Server on a Microsoft domain controller is not supported. Installation of a Package Server on a Microsoft domain controller is not supported.	HOWTO59071
For Notification Server to run properly, you must be able to install (or be prompted to install) ActiveX objects. If your Internet Explorer settings prevent the ActiveX control from running, you see errors when you work with jobs and tasks. This function is by design.	N/A
This error occurs even though the **Show Script in a Normal Window** option is selected. The cause of this error may be a new Windows 2008 security feature called "Session isolation".	N/A

Table 1-64 Things to know about UNIX/Linux/Mac

Information	Article Link
When you push-install the Unix/Linux/Mac agent onto the HP-UX computers that have CSH set as boot-shell for root, links to the agent's binaries location (commands) are created. However, on systems such as HP-UX ia64 11.23-11.31, these binaries or commands cannot be executed in user sessions. In this case, you must specify the absolute path.	N/A

Table 1-64 Things to know about UNIX/Linux/Mac *(continued)*

Information	Article Link
If you attempt to push-install the Symantec Management Agent for UNIX, Linux, and Mac to a computer system that has a secondary shell that is configured in .profile, the installation may fail. The failure is due to a timeout error. The secondary shell is any shell other than the configured shell in `/etc/passwd` for user root in `/etc/profile`, `.profile`, or `.bash_profile`.	N/A
This issue is a system limitation that is caused by Mac OS 10.6 operating system design, and it cannot be overridden. This limitation may affect the commands that SWD/SMF tasks execute, or it may affect Script tasks.	N/A
When you import a .bz2 package into a software component, the command line for installing this package is generated automatically. While this command line works on Linux and Mac computers, it may not work on some HP-UX systems. In this situation, you must manually adjust the command line.	N/A
A package server configuration has an **Alternate Download Location** option. With a Linux package server, you can set this option with a Windows-style path. The path is then converted to a UNIX-style path; for example, `C:\path\` becomes `/path/`. However, a trailing slash is required for proper conversion. If you omit the trailing slash as in `C:\path`, then the path is not converted correctly.	N/A

Table 1-65 Things to know about Network Discovery

Information	Article Link
Symantec Management Platform supports only **Universal Groups** for the cross-domain Active Directory import. Other group types are not supported.	N/A
Use connection profiles to configure the protocols that are used to communicate with network devices.	HOWTO9348
You can set up Symantec Management Platform Security Privileges.	DOC1740
If you schedule a Network Discovery task to run on a recurring basis, you cannot stop that task unless you perform one of the following actions: ■ Delete the task. ■ In the console, under **Manage > Jobs and Tasks**, delete the next scheduled occurrence of the task. This action cancels the schedule.	N/A

Table 1-66 Things to know about Data Connector

Information	Article link
When you import subnets or computers with Data Connector, make sure that you use the following resource lookup keys: ■ For subnets, use **Subnet/Subnet Mask** lookup key. ■ For computers, use **Computer Name/Domain** lookup key.	HOWTO95681 HOWTO95682

Table 1-67 Things to know about SymHelp

Information	Article link
When SymHelp contains the content that can be accessed through HTTP or HTTPS protocols, by default, the Internet Explorer displays only secured content, thereby blocking all unsecured content. To let Internet Explorer display the blocked SymHelp content, do the following: ■ Go to browser security settings and customize it to enable the mixed content display.	kb/2625928 ee264315

Other things to know about Monitor Solution

The following are the things to know about this release.

Table 1-68 Other things to know about Monitor Solution

Issue	Description
SQL policies need to be updated.	After the upgrade to 8.1, all the custom SQL policies that were added before the upgrade need to be updated. To update a policy, do the following: ■ Open the policy and check if the policy is turned on. ■ Click **Save changes**. The data of the updated policies will be encrypted using the FIPS compatible encryption algorithm.

Other things to know about Patch Management Solution

The following are the things to know about this release.

Table 1-69 Other things to know about Patch Management Solution

Issue	Description
Restart and delivery data loss after the upgrade to the latest version of Notification Server.	When you retarget the client computers from the Notification Server version earlier that 8.0 to the latest version of Notification Server, the information about the restart and delivery status of the Symantec Management Agent is lost. For more information, see the KB article INFO3179.
Restart Required to Complete Installation automation policy.	This automation policy generates a report and sends an email if a client computer needs to be restarted to complete the software update installation. This policy only works with Symantec Management Agent 8.0 and later. Older Symantec Management Agent versions are not supported.

Other things to know about Software Management Solution

The following are the things to know about this release.

Table 1-70 Other things to know about Software Management Solution

Issue	Description
Execution Status report has been modified to filter the tasks by name.	**Execution Status** report has been modified to filter the tasks by name if the **Only most recent for Computer** option is selected in the **Software Delivery Instances to Include** drop-down list.
Old **AddRemoveProgram** data class entries are displayed in the Resource Manager after the corresponding software is upgraded on the client computers.	If a client computer software, for which the data is already gathered by the **Collect full inventory** task, is upgraded, old entries in the AddRemoveProgram data class are visible in the Resource Manager, even after running the **Collect full inventory** task on this client computer. Workaround: To fix the issue, run the **Collect full inventory** task on this client computer once again.
Java Update software component is not added into the Software Catalog after running the Software Discovery task.	Java 6 Update software component, which is installed on the client computer, is not added into the Software Catalog after running the Software Discovery task. This happens, because Java 6 Update software component has association with Java(TM) 6 Unmanaged software product, which is added by the Inventory Solution.
If an externally initiated restart is performed during Managed Software Delivery, then the software that is installed after the restart fails.	If an externally initiated restart is performed during Managed Software Delivery, then the software that is installed after the restart fails. The reason the installation fails is that the software starts to install while a user logoff is still pending.

Table 1-70 Other things to know about Software Management Solution *(continued)*

Issue	Description
The support of **Run from server if bandwidth is above some speed** setting is limited in CEM mode.	The usage of this setting on Internet-managed client computers is limited as follows: ■ If the setting is enabled for a Quick Delivery task or a Package Delivery task, these tasks will fail with timeout error, unless the client computer connects remotely or locally with corresponding bandwidth to the Notification Server computer or Package Server, to which it is assigned, before the task timeout period is reached. ■ If the setting is enabled for a Managed Delivery policy, the policy will not run, until the client computer connects remotely or locally with corresponding bandwidth to the Notification Server computer or Package Server, to which it is assigned, before the task timeout period is reached.
Computers in CEM mode cannot be turned on if necessary.	The **Power on computers if necessary** compliance setting is not supported for Internet-managed client computers due to limitations of remote power management technology.
Managed Software Delivery policies and Quick Software Delivery tasks execution requires Symantec Management Agent upgrade.	Due to significant changes in this component, Symantec Management Agent has to be upgraded to version 7.5 in an environment with hierarchy, to execute Managed Software Delivery policies and Quick Software Delivery tasks
Source Path Update execution requires Symantec User credentials.	Source Path Update will only work under Symantec User Credentials.
The status of the Quick Delivery tasks for software resources with EXE files, which contain MSI packages, does not reflect the status of the embedded MSI package installation.	Tasks and policies allow you to use software packages with EXE executable files, which contain MSI components. The logic behind such tasks only monitors the execution of the initial EXE file, which calls the MSI component. Once the embedded MSI is triggered, the result of the task or policy is considered to be successful. This may lead to confusing situations, in case the embedded MSI file fails to complete, particularly, when you use Quick Delivery tasks, which do not utilize detection checks. For example, if you try to install an executable with Adobe Reader in silent mode, using a Quick Delivery task on a client computer running Windows 7 Embedded, the installation may fail, without returning an error code, while the Quick Delivery task status returns successful completion of the executable file. Symantec recommends you to use MSI software packages instead of EXE files and policies with detection checks instead of Quick Delivery tasks, where possible, to make sure receive accurate and detailed information about the software installation process.

Table 1-70 Other things to know about Software Management Solution *(continued)*

Issue	Description
Tasks and policies may fail to access UNC source locations in complex network environments..	Windows Installer Repair task, Quick Delivery task, Package Delivery task and Managed software delivery policy may fail to access the UNC source location, which contains the software package, in an environment, where Notification Server, package server and client computers do not reside in the same domain. To ensure access to such packages, use the agent connectivity credential to connect to download resources. For more information setting up access to the Package Server, see the *Enabling access to a package at a UNC source location* section in the *IT Management Suite Administration Guide*.

Where to get more information

Use the following documentation resources to learn about and use this product.

Table 1-71 Documentation resources

Document	Description	Location
Release Notes	Information about new features and important issues.	The **Supported Products A-Z** page, which is available at the following URL: https://www.symantec.com/products/products-az Open your product's support page, and then under **Common Topics**, click **Release Notes**.
User Guide	Information about how to use this product, including detailed technical information and instructions for performing common tasks.	■ The Documentation Library, which is available in the Symantec Management Console on the **Help** menu. ■ The **Supported Products A-Z** page, which is available at the following URL: https://www.symantec.com/products/products-az Open your product's support page, and then under **Common Topics**, click **Documentation**.

Table 1-71 Documentation resources *(continued)*

Document	Description	Location
Help	Information about how to use this product, including detailed technical information and instructions for performing common tasks. Help is available at the solution level and at the suite level. This information is available in HTML help format.	The Documentation Library, which is available in the Symantec Management Console on the **Help** menu. Context-sensitive help is available for most screens in the Symantec Management Console. You can open context-sensitive help in the following ways: ■ Click the page and then press the F1 key. ■ Use the Context command, which is available in the Symantec Management Console on the **Help** menu.

In addition to the product documentation, you can use the following resources to learn about Symantec products.

Table 1-72 Symantec product information resources

Resource	Description	Location
SymWISE Support Knowledgebase	Articles, incidents, and issues about Symantec products.	Knowledge Base
Cloud Unified Help System	All available IT Management Suite and solution guides are accessible from this Symantec Unified Help System that is launched on cloud.	Unified Help System

Table 1-72 Symantec product information resources *(continued)*

Resource	Description	Location
Symantec Connect	An online resource that contains forums, articles, blogs, downloads, events, videos, groups, and ideas for users of Symantec products.	The links to various groups on Connect are as follows: ■ Deployment and Imaging ■ Discovery and Inventory ■ ITMS Administrator ■ Mac Management ■ Monitor Solution and Server Health ■ Patch Management ■ Reporting ■ ServiceDesk and Workflow ■ Software Management ■ Server Management ■ Workspace Virtualization and Streaming